Investigating the Formation of an Information Security Climate in a Large Vietnamese Construction Company: A Social Network Analysis Approach

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

Duy Pham Thien Dang

Bachelor of Business (Honours), RMIT University

Bachelor of Business (Business Information Systems), RMIT Vietnam

School of Business IT and Logistics

College of Business

RMIT University

Feburary 2018

Declaration

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; any editorial work, paid or unpaid, carried out by a third party is acknowledged; and, ethics procedures and guidelines have been followed.

I acknowledge the support I have received for my research through the provision of an Australian Government Research Training Program Scholarship.

Signed: Duy Pham Thien Dang

Date: February 2018

Acknowledgements

This PhD journey has given me many challenges, yet plenty of enjoyable moments, amazing company, and countless opportunities for me to learn and grow as an academic. I would like to thank those people encountered on this journey, whose advice and support have been extremely valuable. First and foremost, I would like to express my deepest gratitude to my PhD supervisors:

- Dr. Siddhi Pittayachawan, an excellent teacher and a great friend, who has offered me guidance and continuous support throughout my research journey since starting the Honours program. He always encouraged me to step out of my comfort zone and explore novel ways of doing research. Thanks to his constant encouragement, I have developed a passion for and expertise in social network analysis, which contributed to the completion of this PhD thesis.
- Dr. Vince Bruno, a caring supervisor who was always available to share the good and tough times during my research journey. I was able to drop by his office, even without an appointment, to seek his advice for work and personal matters. He also stayed after working hours to discuss research with me, and often reviewed my thesis with me online while I was in Vietnam, in the evening or on his way back home due to the time difference.
- Professor Karlheinz Kautz, a mentor and a father figure with a wealth of experience and knowledge in the information systems field. Words fail to describe how truly grateful I am to have him join the supervisor team in the later stages of my PhD journey. It is my great honour and privilege to become his PhD student, and I have enjoyed the interesting and thought-provoking conversations with him during my candidature.

My special appreciation to professional and academic staff in the School of Business IT & Logistics at RMIT University, especially Professor Caroline Chan, Head of School, and Professor Booi Kam, Professor Alemayehu Molla, Professor Prem Chhetri, Dr. Leon Teo, Dr. Elsie Hooi, Dr. Huan Vo-Tran, and Dr. Konrad Peszynski. These people have given me many research and teaching opportunities, as well as valuable career advice and encouragement during my PhD candidature. I also acknowledge the proofreading service provided by Capstone Editing.

I am grateful to Mr. Lê Bá Thông, General Director of TTT Corporation, and members of the Board of Directors, who have trusted and granted me access to conduct this PhD project in their company. Special thanks to Mr. Đoàn Văn Tùng and Ms. Nguyễn Huỳnh Lan Chi, who have supported me throughout this project. I greatly appreciated the efforts of more than 300 employees at TTT Corporation who have contributed to this project, despite their busy work schedules, through their participation in the research activities.

I would like to thank A/Prof Mathews Nkhoma, Head of School of Business & Management at RMIT Vietnam, who provided me with a workspace and necessary resources at the Vietnam campus during my frequent research visits to Vietnam. I am also thankful to the staff at RMIT Vietnam, especially A/Prof Nguyễn Thanh Thủy, Research Manager, for providing various opportunities to discuss my research.

I owe my utmost gratitude to my Mother, Phạm Thị Thu Thủy, and Father, Đặng Hoàng Dũng, and to my wonderful wife Uyên and her parents, for their unfailing love, patience, and understanding. These people are my source of energy throughout this PhD process, and their continuous support will forever remain my inspiration. I thank them from the bottom of my heart.

Table of Contents

List of Tables

List of Figures

List of Publications

Publications from the thesis

Dang-Pham, D, Kautz, K, Pittayachawan, S, & Bruno, V 2017, 'A canonical action research approach to the effective diffusion of information security with social network analysis', *International Journal of Systems and Society*, vol. 4, no. 2, pp. 22–43 (doi: 2010.4018/IJSS.2017070103).

Dang-Pham, D, Kautz, K, Pittayachawan, S, & Bruno, V 2017, 'Understanding the formation of information security climate perceptions: a longitudinal social network analysis", in *Proceedings of the Australasian Conference on Information Systems (ACIS 2018)*, Universtiy of Tasmania, Hobart, TAS, pp. 1–11. **[ACS Best Paper Award (Third Place)]**

Dang-Pham, D, Pittayachawan, S, & Bruno, V 2017, 'Applications of social network analysis in behavioural information security research: concepts and empirical analysis', *Computers & Security*, vol. 68, pp. 1–15 (doi: 10.1016/j.cose.2017.03.010). **[ERA=A; SJR=Q1]**

Dang-Pham, D, Pittayachawan, S, & Bruno, V 2017, 'Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace', *Information & Management*, vol. 54, no. 5, pp. 625–637 (doi: 10.1016/j.im.2016.12.003). **[ERA=A*; SJR=Q1]**

Dang-Pham, D, Pittayachawan, S, & Bruno, V 2017, 'Exploring behavioral information security networks in an organizational context: an empirical case study', *Journal of Information Security and Applications*, vol. 34 (Part 1), pp. 46–62 (doi: 10.1016/j.jisa.2016.06.002).

Dang-Pham, D, Pittayachawan, S, and Bruno, V 2016, 'Impacts of security climate on employees' sharing of security advice and troubleshooting: Empirical networks', *Business Horizons*, vol. 59, no. 6, pp. 571–584 (doi: 10.1016/j.bushor.2016.07.003).

Dang-Pham, D, Pittayachawan, S & Bruno, V 2015, 'Factors of people-centric security climate: conceptual model and exploratory study in Vietnam', in *Proceedings of the*

Australasian Conference on Information Systems (ACIS 2015), University of South Australia, Adelaide, SA, pp. 1–14.

Dang-Pham, D, Pittayachawan, S & Bruno, V 2015, 'Investigating the formation of information security climate perceptions with social network analysis: a research proposal', in *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2015)*, National University of Singapore, Singapore, pp. 1–10.

Relevant publications during the PhD candidature

Dang-Pham, D and Nkhoma, M 2017, 'Effects of team collaboration on sharing information security advice: insights from network analysis', *Information Resources Management Journal*, vol. 30, no. 3, pp. 58–72 (doi: 10.4018/IRMJ.2017070104).

Dang-Pham, D, Pittayachawan, S, Bruno, V, & Kautz, K 2017, 'Investigating the diffusion of IT consumerization in the workplace: a case study using social network analysis', *Information Systems Frontiers*, pp. 1–15 (doi: 10.1007/s10796-017-9796-5). **[ERA=A; SJR=Q2]**

Dang-Pham, D, Pittayachawan, S, & Bruno, V 2017, 'Investigation into the formation of information security influence: network analysis of an emerging organisation', *Computers & Security*, vol. 70, pp. 111–123. **[ERA=A; SJR=Q1]**

Dang-Pham, D, Pittayachawan, S, & Bruno, V 2017, 'Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace', *Computers in Human Behavior*, vol. 67, pp. 196–206 (doi: 10.1016/j.chb.2016.10.025). **[ERA=B; SJR=Q1]**

Pham, HC, Dang-Pham, D, Brennan, L, & Richardson, J 2017, 'Information security and people: a conundrum for compliance', *Australasian Journal of Information Systems*, vol. 21, pp. 1–16 (doi: 10.3127/ajis.v21i0.1321). **[ERA=A]**

Dang-Pham, D, Pittayachawan, S & Bruno, V 2016, 'Who influences information security behaviours of young home computer users in Vietnam? An ego-centric network analysis approach', in *Proceedings of the Australasian Conference on Information Systems (ACIS 2016)*, Universtiy of Wollongong, Wollongong, NSW, pp. 1–11.

Dang-Pham, D & Pittayachawan, S 2015, 'Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach', *Computers & Security*, vol. 48, pp. 281–297 (doi: 10.1016/j.cose.2014.11.002). **[ERA=A; SJR=Q1]**

Dang-Pham, D, Pittayachawan, S & Bruno, V 2014, 'Towards a complete understanding of information security misbehaviours: a proposal for future research with social network analysis approach', in *Proceedings of the Australasian Conference on Information Systems (ACIS 2014)*, Auckland University of Technology, Auckland, New Zealand, pp. 1–10.

Dang, D. 2014, 'Predicting insider's malicious security behaviours: a general strain theory-based conceptual model', in *Proceedings of the International Conference on Information Resources Management (Conf-IRM 2014)*, Ton Duc Thang University, Ho Chi Minh City, Vietnam, pp. 1–11.

List of Abbreviations

AR	action research
BSP	Business Solutions Provider
CAR	canonical action research
CPR	collaborative practice research
CPM	cyclical process model
ERGM	exponential random graph modelling
GDT	general deterrence theory
HR	human resource
InfoSec	information security
IT	information technology
KPI	key performance indicator
NIST	National Institute of Standards and Technology
PMT	protection motivation theory
RCA	researcher–client agreement
SNA	social network analysis
SAO	stochastic actor-oriented
SAOM	stochastic actor-oriented modelling
TPB	theory of planned behaviour
TTT	TTT Corporation

Abstract

The management of organisational information security (InfoSec) has gained importance due to the rise of new and sophisticated cyberthreats with technical measures alone no longer comprising effective organisational InfoSec. In addition to technical measures, organisations need to transform their employees into InfoSec-aware end-users who actively contribute to the maintenance and improvements of organisational InfoSec. It is imperative to develop a positive InfoSec climate in the workplace where priority of InfoSec-related matters is understood and recognised by all employees.

The concept of an InfoSec climate focuses on the interactions between employees and their work environment, including the InfoSec behaviours performed by colleagues and by direct supervisors. These interactions promote the priority of InfoSec in the organisation. Improving the understanding of these interactions enables scholars and practitioners to design management models and strategies to develop people-centric InfoSec workplaces where employees receive InfoSec-related resources in a positive InfoSec climate. These interactions provide a social network within the workplace and their impact on the formation of an InfoSec climate is the focus of this thesis. Previously, most behavioural InfoSec studies have focused on the cognitive and behavioural aspects of employees as separate individuals.

This thesis investigates the factors and mechanisms that contribute to the formation of an InfoSec climate by conducting a canonical action research (CAR) project in collaboration with a large construction enterprise in Vietnam. The business objective of this CAR project focused on improving the organisation's InfoSec environment. A social network analysis (SNA) approach was used to examine the impacts of employees' networks of InfoSec-related interactions on the formation of their perceptions of an InfoSec climate. The adoption of SNA methods also supported the achievement of the business objective.

The CAR project consisted of four research stages which began with diagnosing InfoSec issues and understanding the critical factors and methods for effective InfoSec implementation in the Vietnamese context. At the end of the diagnosis stage, the project team decided to improve the InfoSec environment through a diffusion of InfoSec knowledge. In the action planning stage, SNA methods were employed to identify influential champions. These champions then received InfoSec training in the action taking stage and carried out the diffusion of InfoSec

knowledge at the end of this iteration. In the evaluation and reflection stage, SNA was performed to quantitatively evaluate the changes in the InfoSec environment and to examine a theoretical model which described the formation of employees' perceptions of the InfoSec climate.

The evaluation's findings indicated that the InfoSec environment of the organisation had achieved the intended improvements, including the selected champions emerging as prominent sources of InfoSec support and InfoSec influence and employees' provision of InfoSec support becoming more active after the champions' diffusion of InfoSec knowledge. The SNA findings further indicated that employees received InfoSec influence from colleagues they trusted and from those that provided them with work advice, organisational updates, personal advice and InfoSec support. Employees' number of InfoSec influencers, department membership and champion status were identified as the factors that facilitated the InfoSec influence between them and contributed to improved perceptions of the InfoSec climate. In addition to the structural mechanisms of the InfoSec influence network, which contributed to InfoSec climate formation, employees' perceptions of colleagues' and direct supervisors' InfoSec behaviours also had different formation mechanisms.

This research provides contributions to practice, theory and methodology. It demonstrates the practical adoption of SNA approach to improve organisational InfoSec, through employing the approach's methods and metrics to evaluate an InfoSec environment and to identify InfoSec champions. The research elaborates on the formation mechanisms of an InfoSec climate and extends theoretical knowledge on this formation process. The examination of theories about networks and social influence also suggests the influential traits of InfoSec champions. The methodological contributions focus on the separate and combined use of SNA methods with the CAR approach to investigate behavioural InfoSec-related phenomena. The research also proposes further improvements to the CAR approach.

Chapter 1: Introduction

Information security (InfoSec) has become a priority for organisations in recent years, accompanying the increasing adoption of technology trends such as cloud computing (Ballabio 2013), mobile devices and consumer technologies for work purposes (Harris, Ives & Junglas 2011; Singh 2012) and big data (Constantine 2014; Everett 2015). In a survey by PwC (2016), 59 per cent of more than 10,000 information technology (IT)/InfoSec executives reported their investment in InfoSec has been affected by the digitalisation of their businesses. In a survey conducted by EY (2017), 53 per cent of 1,735 C-suite leaders and IT/InfoSec executives reported an increased InfoSec budget, yet 87 per cent stated a lack of confidence in their organisation's InfoSec. Reports by other InfoSec institutes have also found a pattern of increased organisational InfoSec budgets over the last three years (Cisco 2017; Filkins 2016; Ponemon Institute 2016).

The recent worldwide increase in InfoSec spending was in response to the growing number of InfoSec threats associated with the adoption of mobile devices and cloud infrastructure, but was also prompted by security concerns regarding employees (Cisco 2017; EY 2017; Ponemon Institute 2016; PwC 2016; Symantec 2017). While the InfoSec threats from the adoption of mobile devices and cloud computing are linked to emerging technology trends and management practices such as Bring Your Own Device (BYOD), IT consumerisation and digitising workplace (Crossler et al. 2014; Harris, Ives & Junglas 2011; Miller, Voas & Hurlburt 2012; Niehaves, Köffer & Ortbach 2012; Thomson 2012; White 2012), InfoSec issues related to employees persist in modern organisations. Employees have been consistently regarded by scholars as the weakest link in organisational InfoSec (Bulgurcu, Cavusoglu & Benbasat 2010a; Crossler et al. 2013; Guo et al. 2011; Ifinedo 2014; Safa, von Solms & Futcher 2016; Sasse, Brostoff & Weirich 2001; Warkentin & Willison 2009). In the context of ongoing worldwide efforts to improve organisational InfoSec, this thesis seeks to develop a practical and novel approach to improve the InfoSec environment through empowering its human-related factors.

1.1 Research Overview

I adopted a canonical action research (CAR) approach and collaborated with a large construction enterprise in Vietnam—TTT Corporation (TTT)—to improve their organisational InfoSec. In doing so, I examined the practical applications of social network analysis (SNA) methods to identify and utilise champions for the diffusion of InfoSec knowledge with the aim to increase employees' provisions of InfoSec support and InfoSec influence in the workplace.

Throughout the thesis I demonstrated the previously unexplored use of SNA methods to investigate the impacts of employees' social networks on their InfoSec perceptions—a factor overlooked by traditional behavioural InfoSec research. In particular, I investigated the factors and mechanisms of the formation process of the InfoSec climate represented by employees' perceptions of their colleagues' and direct supervisors' InfoSec behaviours (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013).

The thesis offers organisational contributions concerning the application of SNA to evaluate and improve an InfoSec environment with network-based interventions by leveraging influential champions to diffuse InfoSec knowledge. Moreover, the thesis extends current knowledge about the determinants of employees' InfoSec influence and the formation process of an InfoSec climate. Finally, this thesis provides methodological recommendations about the combined and separate uses of SNA methods and the CAR approach.

1.2 Research Motivation

The requirements for effective InfoSec management have extended beyond investing solely in technical measures (Anderson & Moore 2009; von Solms 2001), demanding attention be paid to socio-organisational facets of the workplace (Crossler et al. 2013; Willison & Warkentin 2013). Consequently, it is crucial for organisations to gain the knowledge of how employees perceive organisational InfoSec and how they perform InfoSec behaviours (Padayachee 2012; Sommestad et al. 2014).

Recent studies have investigated a wide range of employees' InfoSec perceptions and behaviours such as InfoSec compliance (Herath & Rao 2009a; Lee, Larose & Rifon 2008; Siponen, Pahnila & Mahmood 2007; Siponen, Mahmood & Pahnila 2014; Vance, Siponen & Pahnila 2012) or InfoSec avoidance (Liang & Xue 2010). Other studies have examined reasons for employees' careless mistakes or intentional misbehaviours (D'Arcy & Devaraj 2012; Guo

& Yuan 2012; Siponen & Vance 2010; Workman, Bommer & Straub 2008). These studies identified the antecedents of both desirable and undesirable InfoSec behaviours, thereby enabling practitioners to formulate appropriate strategies to manage these behaviours. However, there remains a gap in the current body of knowledge on behavioural InfoSec which demands further investigation.

The reason for this gap lies in prior studies' focus on InfoSec behaviours and cognition of employees as separate individuals, overlooking the effects and features of the interactions and relationships between employees. Although InfoSec-related interactions and relationships have been examined by some studies, such as employees' sharing of InfoSec advice (Safa, von Solms & Futcher 2016), social learning (Warkentin, Johnston & Shropshire 2011) or social influence (Herath & Rao 2009a; Ifinedo 2014), these interactions and relationships were also conceptualised as employees' cognitive factors. Therefore, the individual employees were the main unit of analysis in these studies.

The features of InfoSec-related interactions and relationships as a network have not been captured by prior studies, resulting in the omission of critical factors such as the roles of employees in these InfoSec-related networks and their social cliques. By shifting the research focus to the interactions and relationships that tie employees together, the effects of individuals' personal characteristics on their interactions or relationships can be identified. This enables holistic examination of InfoSec-related phenomena while accounting for characteristics of both the sender and receiver of an interaction or a relationship, instead of focusing on either of these ends as has been done in previous behavioural InfoSec research (i.e., studying how an individual employee perceives the environment and acts on his or her own perceptions).

By shifting the research focus onto the networks of InfoSec-related interactions and relationships this thesis does not solely aim at filling the current knowledge gap, but undertakes a problematisation approach (Alvesson & Kärreman 2007; Alvesson & Sandberg 2011; Sandberg & Alvesson 2010) to explore new research directions in the behavioural InfoSec field. The problematisation approach provides the method to identify and critically examine the assumptions of predominantly adopted theories, providing a basis for interesting and novel research questions. This problematisation approach will be elaborated on in the next chapter.

Exploring the proposed research directions requires a method to effectively analyse the networks of InfoSec-related interactions and relationships (e.g., provision of InfoSec support and InfoSec influence). SNA methods are most appropriate for analysing these networks (Borgatti, Everett & Johnson 2013; Hanneman & Riddle 2005; Otte & Rousseau 2002). I employed the SNA methods to design the interventions in a CAR project to enhance the InfoSec environment of a collaborating organisation. The potential of using SNA methods for advancing scholarly knowledge was examined by applying these methods to test a theoretical model that described the formation of the collaborating organisation's InfoSec climate. The decision to study the formation of an InfoSec climate as the thesis' focal theoretical interest was in line with the collaborating organisation's business objective, which aimed at improving their employees' perceptions of the InfoSec environment. The perceptions of InfoSec climate describe how employees perceive their colleagues and direct supervisors' InfoSec behaviours (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013). The motivations for this CAR project were, therefore, influenced by the collaborating organisation's business objective.

The research project was conducted in Vietnam, a developing country in Southeast Asia. In terms of internet penetration, Vietnam was ranked 13th in the world in 2016 with 52 per cent of the country's population having access to the internet (Internet Live Stats 2016). However, the current InfoSec landscape in Vietnam requires urgent attention. Vietnam was among the top five countries most vulnerable to computer viruses (Kaspersky 2014). A recent whitebook on IT in Vietnam (Vietnam MIC 2014) reported that only 30 per cent of organisations in the country had implemented InfoSec policies and protective measures. In 2016 and 2017, numerous InfoSec incidents impacted companies and crucial infrastructures in Vietnam including the country's international airport (Blake 2016; Lich 2016; Tuoi Tre News 2017). Recently, the Vietnamese Minister of Information and Communication pledged the dedication of resources and support until 2020 to improve the country's IT and InfoSec infrastructures (VietNamNet Bridge 2017). That InfoSec-related topics are pressing issues to organisations in Vietnam further motivated this thesis to explore the practical applications of SNA methods as an effective and efficient tool to improve organisational InfoSec in Vietnam.

1.3 Research Scope and Objectives

1.3.1 Research Objectives

I employed a CAR approach which pursues two types of objectives—scholarly and business objectives. The scholarly objectives were to investigate the formation of an InfoSec climate and explore the applications of SNA methods for improving organisational InfoSec. The business objective of the collaborating organisation was to improve their InfoSec environment.

1.3.2 Research Context

For this CAR project, I collaborated with an industry partner, TTT[1], one of the largest construction enterprises in Vietnam in operation since 1992. TTT focuses on delivering interior design and fitting to multinational clients in Vietnam and Myanmar, while its sister company, Gamma Chairs[2], specialises in manufacturing and exporting high-quality furniture worldwide.

TTT attracts 100 to 300 projects annually and employs more than 300 permanent full-time employees at three offices in Ho Chi Minh City and Ha Noi, and more than 800 skilled workers at the factory complex and various construction sites in Vietnam and Myanmar. TTT is respected by clients and competitors as an innovative construction enterprise in the interior design and fitting market in Vietnam. TTT prides itself on being the first construction company in Vietnam to adopt technologies such as customer relationship management and enterprise resource planning systems to support its operations. Most recently, the company pioneered the emerging eco-friendly architecture practices in Vietnam.

Due to rapid growth, the top management at TTT started to improve the company's digital operations and corporate image. In doing so, they decided to pursue excellence in InfoSec governance—InfoSec issues, which included employees' inefficient and insecure use of confidential information and IT applications, had been identified by their staff. For example, the disorganised files and folders on the company's servers can hinder critical business processes such as project bidding and increase the risk of leaking confidential information. When I approached TTT and presented my thesis proposal, the top management found the

[1] http://www.tttcorporation.com

[2] http://www.gammachairs.com.vn

proposal aligned with their business objectives and agreed to collaborate with me in this research project.

1.4 Research Questions

In line with the research objectives formulated above, this thesis seeks to answer the following research questions:

> **RQ1:** What are the factors and mechanisms that contribute to the formation of an InfoSec climate?
>
> **RQ2:** How can SNA methods be used for improving organisational InfoSec?

1.5 Research Contributions

The contributions of this thesis fall into three groups, 1) organisational contributions, 2) theoretical contributions and 3) methodological contributions.

This thesis produced organisational improvements in the InfoSec environment at TTT by increasing the provision of InfoSec support and InfoSec influence between employees. SNA methods were applied to conduct a risk assessment to quantitatively evaluate the InfoSec environment and to identify influential champions for the diffusion of InfoSec knowledge. TTT benefitted from the research, including through improved understanding of InfoSec implementation and receiving the materials and procedures developed from this thesis as a starting point for future InfoSec improvements. TTT also received a group of experienced champions who can continue to diffuse InfoSec knowledge in the future. Overall, the thesis demonstrated the applications of SNA methods to improve InfoSec environment with network-based interventions and provided the selection criteria for appointing influential InfoSec champions.

The thesis offered theoretical contributions by extending current knowledge about the determinants of InfoSec influence and about the mechanisms and factors that contributed to the formation of InfoSec climate. Specifically, I applied SNA methods to identify employees' background characteristics and socialisation that increased their likelihood to exert InfoSec influence over each other. By doing so, I examined the theory of social power bases (Raven 2008) in the InfoSec context and advanced knowledge about the selection criteria for InfoSec champions—a neglected and under-researched topic with important implications. I further

explored the forming mechanisms of an InfoSec climate, offering explanations beyond the theoretical relationships between employees' socialisation, social influence and climate perceptions (Ashforth 1985). Findings from SNA revealed the specific types of socialisation that indirectly contributed to the formation of an InfoSec climate through facilitating InfoSec influence between employees. Moreover, the InfoSec influence network had structural mechanisms which affected the occurrence of InfoSec influence, and employees' climate perceptions were also found to have unique and changing tendencies over time.

Methodological contributions concerning the combined and separate uses of the CAR approach and SNA methods were drawn from my reflection on the CAR process. I found that SNA methods can enhance the effectiveness and rigour of the CAR approach by helping researchers diagnose the organisational situations, design network-based interventions and provide network measures to quantitatively evaluate the intervention's effectiveness. The use of SNA methods further facilitates action researcher–research client collaboration via the effective communication of network visualisations. I further compared the CAR approach with the collaborative practice research (CPR) approach (Mathiassen 2002) and proposed improvements to the CAR approach based on this comparison and on my reflection of the CAR project.

1.6 Organisation of the Thesis

This thesis is organised into nine chapters, illustrated in Figure 1.1 and summarised below.

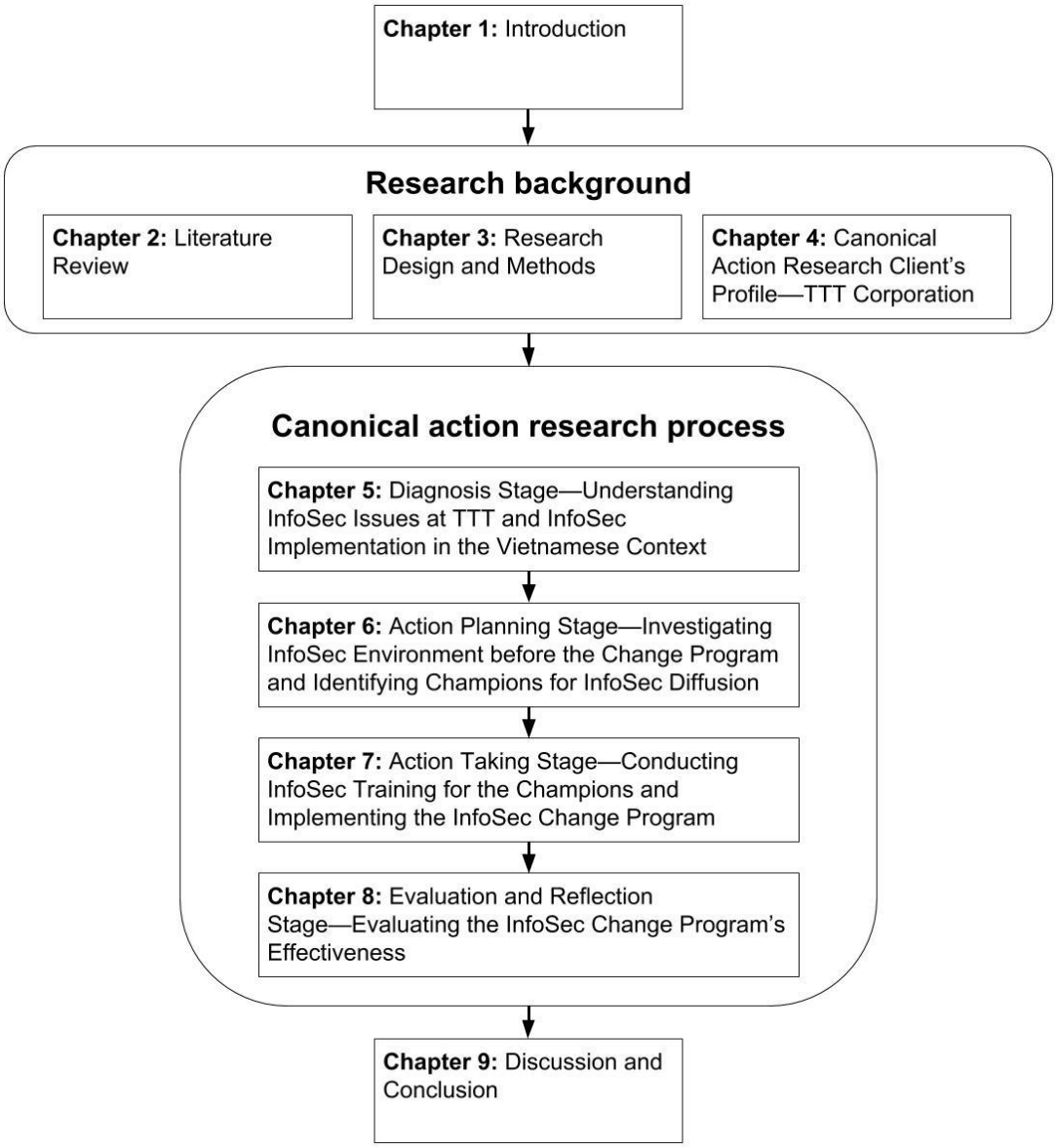


Figure 1.1. Thesis Structure

Chapter 1 introduces key elements such as research context, motivation, scope and objectives and research questions. Chapter 2 reviews the extant literature with a focus on employees' InfoSec behaviours and perceptions. The chapter also explains the problematisation approach that motivates and shapes the thesis' research direction. Chapter 3 describes the research design and methods, focusing on the adoption of the CAR approach and the SNA methods. Chapter 4 presents a detailed profile of TTT, the collaborating industry partner in this CAR project. The chapter also discusses the initial meeting between myself and TTT's stakeholders from which the joint project properly commenced. Together, Chapters 2 to 4 establish the theoretical background and context of this thesis.

Chapter 5 describes the diagnosis stage of the CAR project consisting of two research actions. First, I performed a risk assessment with the department managers at TTT to diagnose the InfoSec issues in the workplace. Second, I conducted a case study with six external InfoSec experts in Vietnam to understand the critical factors and methods for InfoSec implementation in the Vietnamese context. These two actions were carried out as preparatory steps which provided feedback to the design of the InfoSec change program for TTT.

Chapter 6 presents the action planning stage of the CAR project, where the decision and actions to identify the influential champions for the InfoSec change program were taken in consideration of the project's situation. At the end of this stage, 50 champions were identified using SNA methods and appointed for the InfoSec change program. Moreover, the networks of the provision of InfoSec support and InfoSec influence before the change program were analysed as a baseline for the evaluation of improvements.

Chapter 7 describes the action taking stage of the CAR project, where the appointed champions received the InfoSec training to equip them with the necessary skills and knowledge for the diffusion of InfoSec knowledge to colleagues in their departments.

Chapter 8 presents the evaluation and reflection stage of the CAR project, which took place four months after the diffusion of InfoSec knowledge launched at the end of the action taking stage. This evaluation and reflection stage evaluated the changes in the networks as representative of the provision of InfoSec support and InfoSec influence after the change program. I also performed a longitudinal SNA to explain the formation of employees' InfoSec climate perceptions at TTT.

Chapter 9 discusses the CAR project's research contributions, grouped into three categories—organisational contributions, theoretical contributions and methodological contributions concerning the combined and separate uses of the CAR approach and the applied SNA methods.

Chapter 2: Literature Review

This chapter reviews the relevant literature and introduces the major concepts, theories and frameworks in the behavioural InfoSec field. The chapter begins a review of the development of the InfoSec research field from solely focusing on technical measures to aiming to achieve effective InfoSec governance of all factors related to people, processes and technology. The theories that explain several types of employees' InfoSec behaviours are then reviewed and emerging trends in the behavioural InfoSec research field are discussed. The chapter then discusses my adoption of the problematisation approach (Alvesson & Sandberg 2011) to explore new research directions in this field. The knowledge gained from this literature review combined with the problematisation process motivated an investigation into the formation of InfoSec climate by applying SNA methods. The structure of this chapter is illustrated in Figure 2.1.

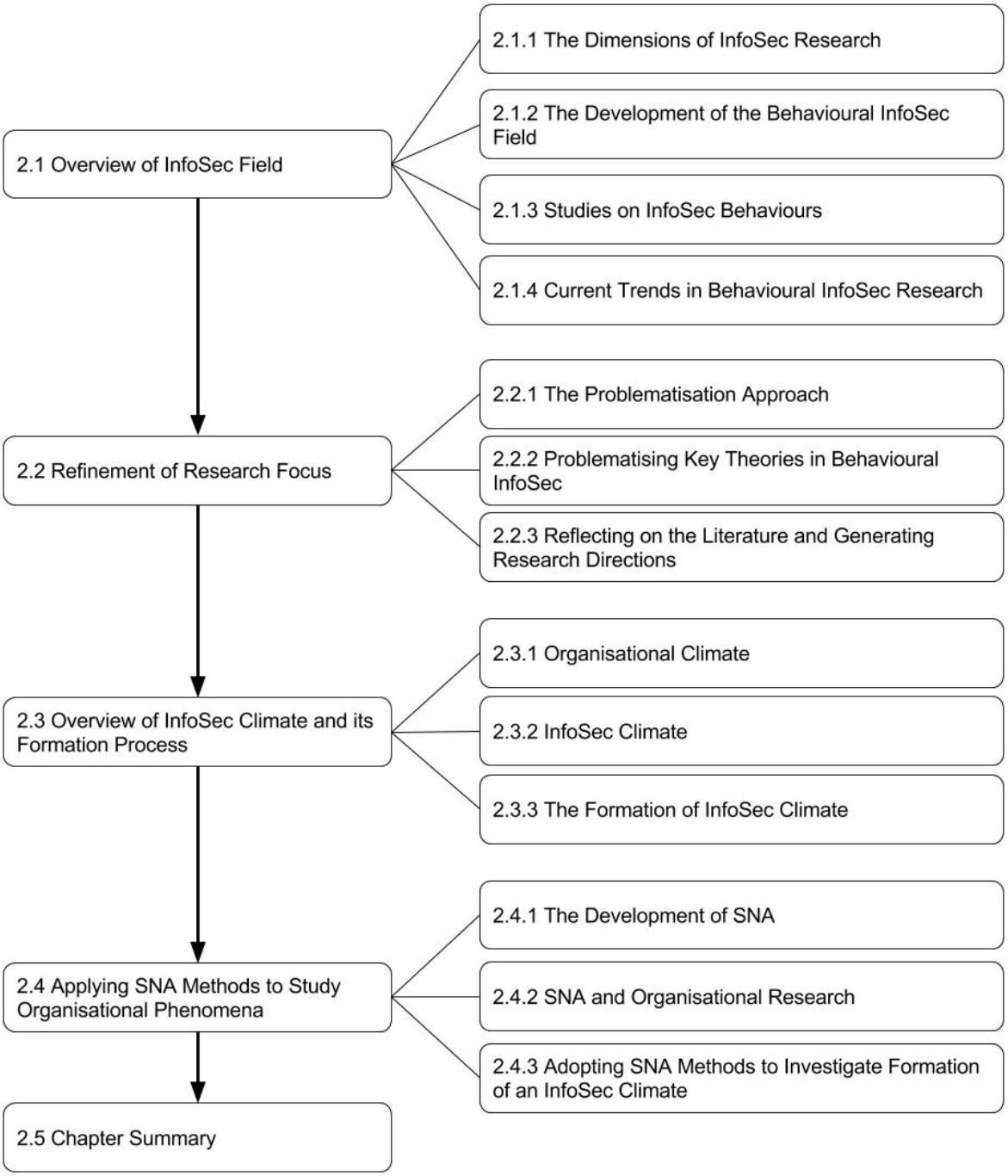


Figure 2.1. Structure of Chapter 2

2.1 Overview of InfoSec Field

The United States National Institute of Standards and Technology (NIST) defines InfoSec as 'the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability' (Kissel 2013, p. 94). InfoSec practitioners and researchers have also widely referred to the confidentiality, integrity and availability triad as a canonical definition of

InfoSec, referring to the objective of preserving these three facets of information (Anderson 2003; Dhillon & Torkzadeh 2006; Huang, Lee & Kao 2006; ISO 2017; Parsons et al. 2010; Saint-Germain 2005; von Solms & van Niekerk 2013; Stanton et al. 2005). Moreover, InfoSec is often interpreted as concerning risk management activities (Blakley & Mcdermott 2002; Dhillon & Torkzadeh 2006).

The definition of InfoSec has changed over the past decade as the InfoSec research field has grown in importance and expanded its domains. For example, von Solms and von Solms (2005) state that the scope of InfoSec has grown beyond the protection of data, information and software to include critical business and legal implications. Similarly, InfoSec research is no longer considered a discipline solely focused on InfoSec technologies, but one that also comprises topics related to economics, psychology and management areas (Anderson & Moore 2009; Crossler et al. 2013). The various dimensions of InfoSec research are discussed in the next section.

2.1.1 The Dimensions of InfoSec Research

Von Solms (2001) identified 13 dimensions of the InfoSec discipline—strategic/corporate governance, governance/organisational, policy, best practice, ethical, certification, legal, insurance, personnel/human, awareness, technical, measurement/metrics and audit. Da Veiga and Eloff (2007) developed an InfoSec governance framework that covered six major InfoSec domains—leadership and governance, security management and organisation, security policies, security program management, user security management and technology protection and operations. Wu and Saunders (2011) compared da Veiga and Eloff's (2007) work with the framework described by the NIST's Special Publication 800 series and incorporated the budget dimension into the existing InfoSec framework.

Zafar and Clark (2009) reviewed and matched the InfoSec research topics published in the Basket of Eight's information systems journals with the IBM Information Security Framework (IBM 2006). They then categorised InfoSec research into nine themes—InfoSec governance, privacy, threat mitigation, transaction and data integrity, identity and access management, application security, physical security, personnel security and InfoSec economics (Zafar & Clark 2009). Blake and Ayyagari (2012) conducted text analysis to identify the topics of InfoSec research by examining publications' contents. Based on the keywords derived from these publications, Blake and Ayyagari (2012) found 10 InfoSec research topics—security

design and management, confidentiality and integrity, behavioural aspects of security, user-level security, preventive and detective controls, database security, assessment, research methodology, information protection and reuse and privacy. Most recently, Silic and Back (2014a) combined Zafar and Clark's (2009) InfoSec themes with the ISO27002 model and determined 13 InfoSec research themes (shown in Table 2.1).

Table 2.1. InfoSec Research Themes

Main theme	Sub-themes	
Risk assessment	Risk analysis	Risk estimation
	Risk identification and management	Risk evaluation
Privacy	Policy, practices and controls	Data, rules and objects
	Privacy and information management strategy	
Information security governance	Strategy and information security policy	Information security advisory
	Governance structure	
	Framework and standards	
Asset management	Site management	Physical asset management
Human resources security	Workforce security	Workforce education
	Organisational culture	
Physical and environmental security	Physical asset management	Deterrence
	Environmental security	Detection
	Identification	
	Human response	
Communications and operations management	Operational procedures and responsibilities	System planning and acceptance
	Third party delivery management	
Access control	Identity proofing	Identity lifecycle management
	Access control	
Information systems acquisition, development and maintenance	Systems development life cycle	Application development environment
	Protocols	
Information security incident management	Network segmentation and boundary protection	Content checking
	Vulnerability management	Incident management
Business continuity management	Business Process transaction security	Message protection
		Secure storage
	Database security	Systems integrity
		Knowledge management
Compliance	Compliance program	Standards, laws and regulations
	Information security policies	
Economics	Information security investment	Consumer choice
		Innovation
		Marketing

Adopted from Silic and Back (2014a, p. 290).

Overall, there are several overlapping InfoSec domains and dimensions in the previous research frameworks and industry standards. Von Solms (2006) summarises the development of the InfoSec field as having progressed through four 'waves'. The first wave focused on the technical InfoSec issues and their preventive measures, the second wave addressed the policies and management of organisational InfoSec, the third wave covered best practices and emphasised the development of InfoSec culture, and the fourth wave focused on developing effective InfoSec governance frameworks that oversee all InfoSec-related matters (von Solms 2006). Based on four major InfoSec issues—access to InfoSec, secure communication, security management and development—Siponen and Oinas-Kukkonen (2007) found InfoSec research that contributed to these four issues fall into the organisational, conceptual and technical levels. The organisational level concerns aspects of human employees such as their behaviours and the policies to manage these employees. The conceptual level focuses on implementation-independent specification for InfoSec such as the techniques for modelling InfoSec constraints. The technical level addresses the implementation of technical measures such as encryption algorithms (Siponen & Oinas-Kukkonen 2007).

An important dimension of InfoSec research is end-users. The management of end-users' InfoSec awareness and compliance with InfoSec policies is an integral part of InfoSec governance, which is the focus of the fourth wave development of the behavioural InfoSec field (von Solms 2006). Studies concerning end-user InfoSec contribute to the organisational level of workplaces' InfoSec (Siponen & Oinas-Kukkonen 2007). The research theme focusing on end-user InfoSec is mentioned across research frameworks and industry standards under the names of personnel/human (von Solms 2001), user security management (da Veiga & Eloff 2007), personnel security (Zafar & Clark 2009), people (Wu & Saunders 2011) and human resources security (Silic & Back 2014a).

The research domain of end-user InfoSec is complex, containing various topics on end-users' psychology and behaviours (Anderson & Moore 2009; Silic & Back 2014a; da Veiga & Eloff 2007; Wu & Saunders 2011) and it has emerged as a critical subfield of InfoSec research (Crossler et al. 2013). This thesis, with the aim of understanding and influencing the formation of an InfoSec climate through the applications of SNA methods to enhance employees' provision of InfoSec support and InfoSec influence, contributes to this behavioural InfoSec research field.

2.1.2 The Development of the Behavioural InfoSec Field

End-users had been examined in the context of InfoSec before being recognised as a critical domain of InfoSec research and InfoSec governance. For example, end-users' InfoSec behaviours were categorised as a form of organisational InfoSec threats, which can be internal (e.g., disgruntled employee, bad data entered and modified data) and external (e.g., hackers and competitors) (e.g., Loch, Carr & Warkentin 1992; Loch & Carr 1991; Wilson, Turban & Zviran 1992; Wood & Banks Jr 1993). Insider threats received the most attention at that time and Straub (1990) developed the well-known general deterrence theory (GDT) in the InfoSec context, that internal InfoSec violations can be deterred by end-users' perceptions of the sanctions for their potential violations. Goodhue and Straub (1991) proposed and tested a theoretical model for end-users' psychological satisfactoriness of InfoSec measures, finding little about the predictors of such satisfactoriness. The theoretical models proposed by Straub (1990) and Goodhue and Straub (1991) were the first attempts to understand end-users' perceptions of InfoSec-related matters.

End-users' psychological factors and processes related to InfoSec gradually received more attention from practitioners and researchers. Of these factors, end-users' InfoSec awareness emerged as a key topic discussed in many academic publications and industry guidelines (e.g., Gaunt 2000; Hawkins, Yen & Chou 2000; Guttman & Roback 1995; Sasse, Brostoff & Weirich 2001; Siponen 2000a, 2000b, 2001; Thomson & von Solms 1998; Wood 2000). Kabay (1994) looked beyond insider threats and discussed a variety of psychological factors and processes (i.e., persuasion, compliance, group and prosocial behaviours) and suggested taking these factors and processes into consideration when implementing InfoSec policies. Harrington (1996) found that codes of ethics could affect specific InfoSec abuses (e.g., sabotage, fraud and viruses) and suggested InfoSec managers implement ethics codes to strengthen their effects through top management support and continuously reminding end-users about the consequences of InfoSec abuses. Adams and Sasse (1999) argued that end-users should not be viewed as the enemies of organisational InfoSec and emphasised user-centred InfoSec practices to motivate end-users' cooperation in maintaining organisational InfoSec.

Dhillon and Backhouse's (2001) literature review called for more research on the socio-organisational concepts related to InfoSec. End-user InfoSec awareness remained an under-researched area of human-related InfoSec concepts. From 2000 onwards, theoretical frameworks and models for determining the socio-organisational factors of end-users' InfoSec

behaviours were developed and validated, enriching the knowledge on this area (e.g., Aytes & Connolly 2004; Chan, Woon & Kankanhalli 2005; Doherty & Fulford 2005; Leach 2003; Lee, Lee & Yo 2004; Schultz 2002; Stanton et al. 2003). Of particular importance was Stanton et al.'s (2005) research, which classified InfoSec behaviours into six types according to end-users' expertise (expert or novice) and their intention (malicious, neutral or benevolent), the taxonomy of which is illustrated in Figure 2.2.

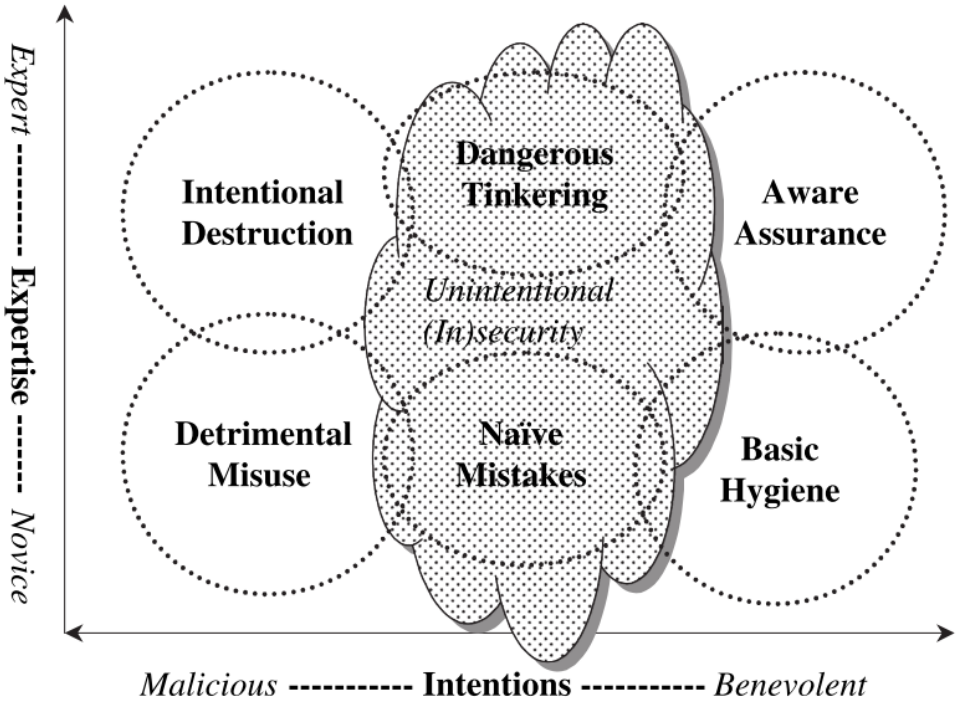


Figure 2.2. Taxonomy of End-Users' InfoSec Behaviours

Adopted from Stanton et al. (2005, p. 127).

InfoSec behaviours can be intentional destruction or detrimental misuse, dangerous tinkering or naive mistakes, and aware assurance or basic hygiene, depending on end-users' level of technical skills (Stanton et al. 2005). Stanton et al. (2005) provided several examples for each of these InfoSec behaviours, such as sabotage or stealing data (intentional destruction), sending spam messages (detrimental misuse), configuring company's network (dangerous tinkering), setting weak passwords (naive mistakes), InfoSec compliance (basic hygiene) and notifying InfoSec vulnerabilities (aware assurance). Based on this taxonomy of end-users' InfoSec behaviours, future research can focus on identifying the antecedents and consequences of each type of InfoSec behaviours.

2.1.3 Studies on InfoSec Behaviours

From 2005 onwards, a substantial number of studies identified the antecedents and consequences of end-users' InfoSec perceptions and behaviours contributing to the effective management of InfoSec. Most studies emphasised end-users' compliance or compliance intention, while some investigated InfoSec violations or intention to commit InfoSec abuses. For example, Siponen, Pahnila and Mahmood (2007) determined the antecedents of end-users' intention to comply and actual compliance. These antecedents were end-users' perceptions of the InfoSec threats, perceived protective measure's effectiveness (i.e., response efficacy), self-efficacy and perceived sanctions. Further research (Pahnila, Siponen & Mahmood 2007) identified end-users' attitude towards InfoSec, normative beliefs, perceived facilitating conditions, habits and rewards as additional factors of actual compliance and compliance intention. These findings were replicated and expanded on by later studies (Bulgurcu, Cavusoglu & Benbasat 2010a; Herath & Rao 2009a, 2009b; Johnston & Warkentin 2010; Lee, Larose & Rifon 2008; Ng, Kankanhalli & Xu 2009; Son 2011; Vance, Siponen & Pahnila 2012). Other factors contributing to end-users' InfoSec compliance and compliance intention were also determined, such as moral reasoning and values (Myyry et al. 2009), national culture (Dinev et al. 2009), management support (Posey, Roberts et al. 2011), perceived technical protection (Zhang, Reithel & Li 2009) and social learning (Warkentin, Johnston & Shropshire 2011).

Alongside the focus on predicting InfoSec compliance and compliance intention, other types of end-users' InfoSec behaviours and perceptions were investigated. For example, researchers explored characteristics of InfoSec policies and their impacts on end-users' engagement with policies (Boss et al. 2009; Bulgurcu, Cavusoglu & Benbasat 2010b; Foltz, Schwager & Anderson 2008; Shaw et al. 2009). Liang and Xue (2010) examined the effects of end-users' threat and coping appraisals on their InfoSec avoidance behaviour, and Rhee, Kim and Ryu (2009) focused on the antecedents of self-efficacy and its impacts on end-users' technical InfoSec practice, intention to strengthen InfoSec and care for InfoSec behaviours.

With regard to undesirable InfoSec behaviours, Workman, Bommer and Straub (2008) found that threat and coping appraisals can reduce end-users' omission of InfoSec measures. D'Arcy and Hovav (2008) and D'Arcy, Hovav and Galletta (2009) investigated end-users' InfoSec misuse and found that InfoSec training and monitoring, InfoSec awareness, moral judgement, self-efficacy and virtual status deterred such misuse and its behavioural intention. Hovav and

D'Arcy (2012) found similar findings, but the results were varied across the American and Korean samples, suggesting the impact of cultural values on deterrent effects. Further, studies have identified the antecedents of malicious and non-malicious InfoSec misbehaviours, such as perceived benefits (Hu et al. 2011), neutralisation techniques (Siponen & Vance 2010), perceptions of organisational justice and computer monitoring (Posey, Bennett et al. 2011), perceived lack of attributed trust (Posey, Bennett & Roberts 2011), attitude, workgroup norm, perceived risks and sanctions (Guo et al. 2011) and self-justification (Kajtazi et al. 2013).

2.1.4 Current Trends in Behavioural InfoSec Research

By 2012, the behavioural InfoSec field had achieved some level of maturity as systematic reviews and opinion articles begun to appear and consolidate research findings within the field (e.g., Crossler et al. 2013; Guo 2013). For example, D'Arcy and Herath (2011) synthesised prior researches adopting GDT (Straub 1990) which had produced inconsistent findings about the deterrent effects on InfoSec misbehaviours, and D'Arcy and Herath (2011) suggested exploring contingency variables to explain such inconsistency.

Padayachee (2012) forwarded a taxonomy which summarised the factors motivating InfoSec compliant behaviours. This taxonomy followed self-determination theory's (Deci & Eghrari 1994; Gagné & Deci 2005) premises that human behaviours are driven by the five types of motivation—external regulation, introjection, identification, integration and intrinsic motivations (see Figure 2.3).

Amotivation describes the state of lacking motivations which leads to having no intentions for performing behaviours (Gagné & Deci 2005). People feel motivated and develop behavioural intentions when they realise rewards and punishments (i.e., external regulations), while others may feel motivated to take actions as their self-esteem and ego are involved in performing the tasks (i.e., introjected regulations).

It must be noted that people motivated by introjected regulation are still controlled by a form of extrinsic motivation (e.g., performing a behaviour because that behaviour makes the person feel worthy) (Gagné & Deci 2005). With identified regulation people have greater freedom as they are motivated to perform behaviours which match their goals and identities (e.g., being a doctor implies having to take care of patients). Moreover, people motivated by integrated regulation fully understand that their behaviours are integral parts of their personal identities (e.g., people who work as nurses while being comfortable with taking care of others in general)

(Gagné & Deci 2005). Opposite to amotivation is intrinsic motivation, the state of being motivated to perform behaviours solely by the enjoyment and autonomy of doing so. The enjoyment in performing behaviours distinguishes intrinsic motivation from integrated motivation (Gagné & Deci 2005).

Based on Gagné and Deci's (2005) self-determination theory, Padayachee's (2012) taxonomy categorised the antecedents of InfoSec behaviours into extrinsic motivation (e.g., deterrence, rewards, social climate, threat and coping appraisals) and intrinsic motivation (e.g., commitment, competence and ethical). Further, amotivation (e.g., apathy, resistance, low self-control and incompetence) can lead to undesirable InfoSec behaviours (Padayachee 2012).

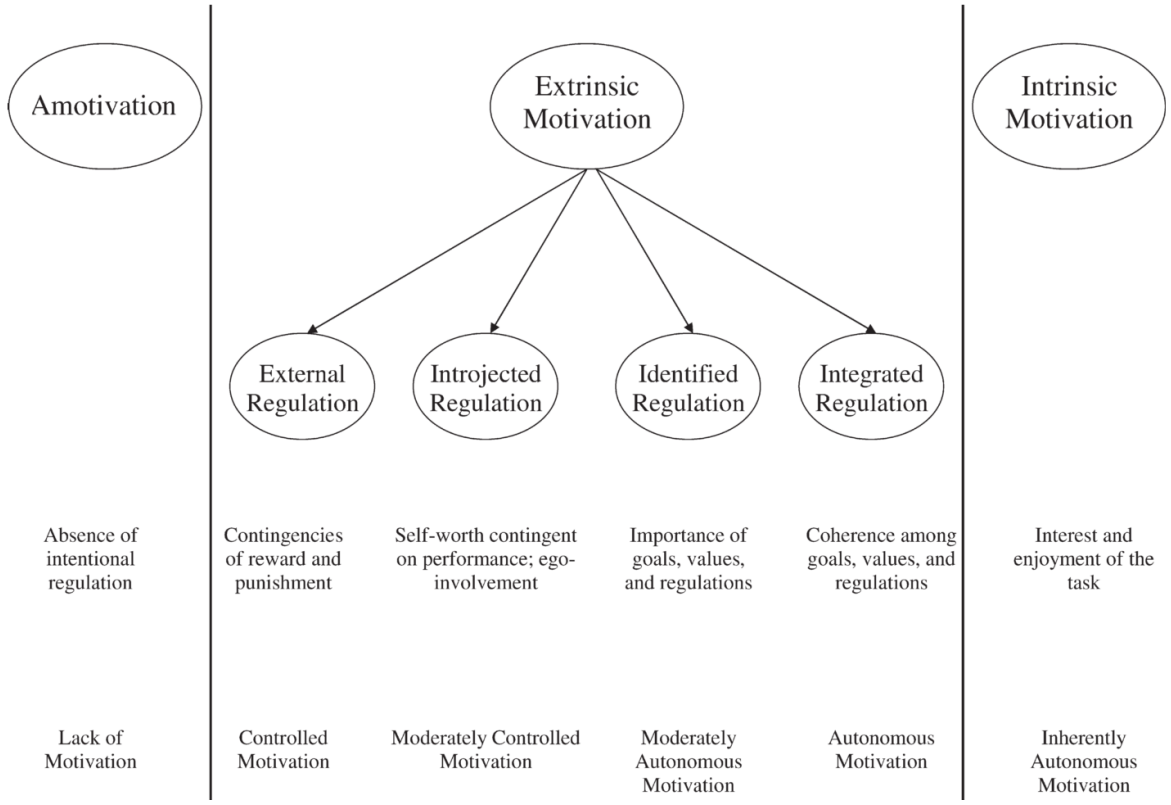


Figure 2.3. The Self-Determination Continuum

Adopted from Gagné and Deci (2005, p. 336).

Sommestad et al. (2014) and Silic and Back (2014a) both conducted systematic InfoSec literature reviews, with the former focused specifically on behavioural InfoSec. Sommestad et al. (2014) produced a list of the best predictors of InfoSec compliance and noncompliance (actual and intention to perform) (i.e., absolute Beta coefficient of impact on InfoSec compliance and misuse ≥ 0.25) and worst predictors (i.e., absolute Beta coefficient of impact ≤ 0.10), as summarised in Table 2.2.

Table 2.2. Predictors of Compliance and Noncompliance (Actual and Intention to Perform)

	Actual behaviour		Intention to perform behaviour	
Predictor	**Compliance**	**Incompliance**	**Compliance**	**Incompliance**
Attitude			8	2
Perceived behavioural control			1	1
Descriptive norm			1	
Subjective norm			8	2
Intention to comply	2			
Intention to misuse		1		
Perceived celerity of sanctions				1
Perceived certainty of sanctions	1		2	2
Perceived severity of sanctions	1		2	2
Perceived cost of noncompliance	1		1	
Self-efficacy	2		5	
Response cost			2	
Response efficacy			4	
Perceived benefits of noncompliance	1		2	1
Perceived vulnerability			3	
Perceived severity of incident			2	
Threat appraisal			1	
Attachment				1
Involvement				1
Organisational commitment			1	1
Perceived extrinsic benefits				1
Perceived formal risk				3
Perceived informal risk				4
Perceived intrinsic benefits				1
Perceived risk of shame				3
Awareness program				1
Computer monitoring				1
Conservation	1		1	
Conventional reasoning	1		1	
Habits			1	
InfoSec policies				1
InfoSec policy fairness			1	
InfoSec policy quality	1		1	
Moral beliefs				3
Neutralisation				2
Openness to change	1		1	
Perceived identity match				1
Perceived InfoSec climate	1			
Perceived justice of punishment			1	
Perceived legitimacy	1			

Perceived usefulness			1		
Perceived value congruence	1				
Preventive security software					1
Satisfaction			1		
Self-defence intention		1			
Visibility			1		

Adopted from Sommestad et al. (2014, pp. 52–56). The table contains 46 variables extracted from 29 studies conducted between 1996 and 2011 which Sommestad et al. (2014) deemed acceptable for inclusion in their review. The figures indicate the number of studies that examined these variables.

Sommestad et al.'s (2014) and Padayachee's (2012) reviews both contained three theoretical models predominantly adopted by prior studies—the theory of planned behaviour (TPB) (Ajzen 2011a), GDT (Straub 1990) and protection motivation theory (PMT) (Rogers 1975). Less commonly adopted theories were social control theory (Hirschi 1969) and rational choice theory (Paternoster & Simpson 1996). The literature reviews focusing on InfoSec behaviours conducted by Lebek et al. (2014) and Warkentin and Mutchler (2014) confirmed TPB, GDT and PMT as the key theories most frequently adopted in the behavioural InfoSec field.

While several studies from 2011 onwards continued to examine and extend the predominantly adopted theoretical models (Burns et al. 2017; Hanus & Wu 2016; Ifinedo 2014; Siponen, Mahmood & Pahnila 2014; Sommestad, Karlzén & Hallberg 2015a, 2015b; Vance, Siponen & Pahnila 2012; Warkentin et al. 2016), others explored the contributing factors of InfoSec behaviours which reflect more of end-users' personal characteristics. For example, Kajzer et al. (2014), Shropshire, Warkentin and Sharma (2015), McCormac et al. (2016) and Öğütçü, Testik and Chouseinoglou (2016) investigated end-users' unique personalities and their impacts on InfoSec perceptions and behaviour.

A closer examination of current trends reveals another change of focus in the behavioural InfoSec field; there is now more focus on end-users' interactions with the InfoSec environment. Willison and Warkentin (2013) adjusted the security action cycle originally developed by Straub and Welke (1998) to add 'pre-kinetic events'. The original security action cycle (Straub & Welke 1998) described four security actions—deterrence, prevention, detection and remedies—shown in Figure 2.4.

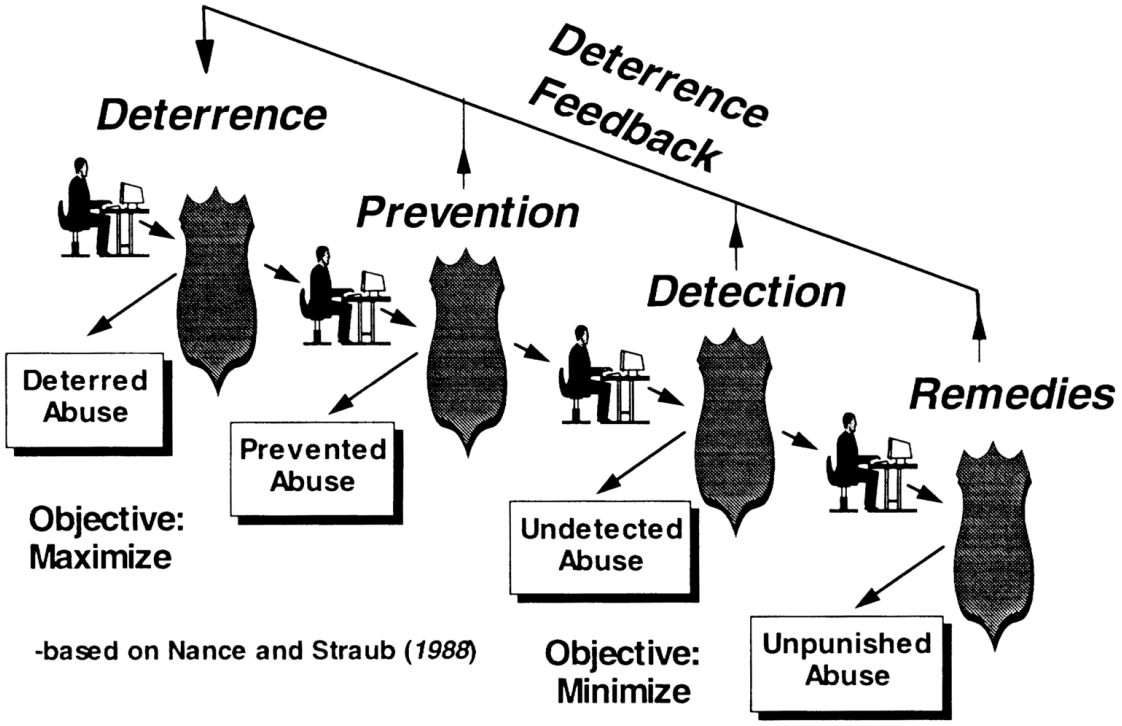


Figure 2.4. Security Action Cycle

Adopted from Straub and Welke (1998, p. 446).

The adjustment of the security action cycle proposed by Willison and Warkentin (2013) added the pre-kinetic events component before the deterrence action (shown in Figure 2.5). They explained that pre-kinetic events can result from the interaction between employees and their organisation, including employees' positive perceptions of a workplace where potential perpetrators do not have any motives to commit InfoSec violations. Pre-kinetic events also include the negative perception of organisational injustice, disgruntlement or dissatisfaction and neutralisation (i.e., mechanisms of moral disengagement that justify employees' violations) which can develop the intention to commit InfoSec violations (Willison & Warkentin 2013).

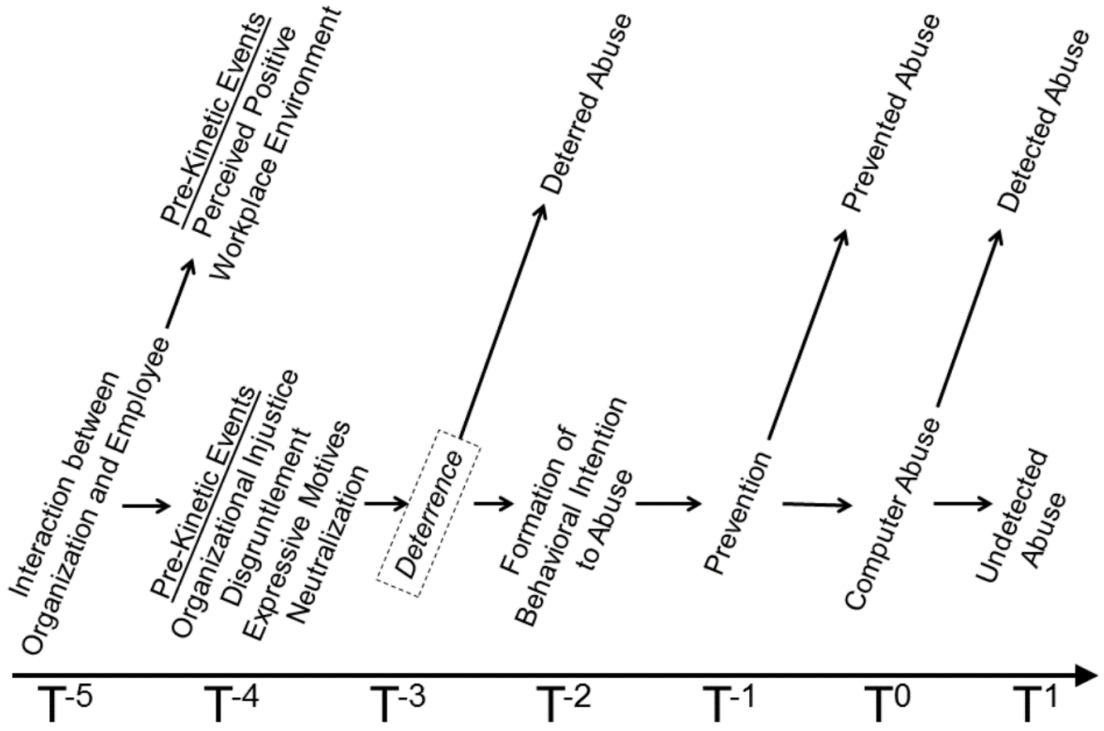


Figure 2.5. Extended Security Action Cycle

Adopted from Willison and Warkentin (2013, p. 5).

In line with Willison and Warkentin's (2013) research, end-users' perceptions of organisational injustice under the work environment's effects were investigated by other studies (Posey, Bennett & Roberts 2011; Posey, Bennett et al. 2011). These studies found that various types of perceived organisational injustice can result from unjust computer monitoring and unpredictable management style, leading to computer abuse. Baskerville, Park and Kim (2014) and Kim, Park and Baskerville (2016) examined potential perpetrators' evaluation of their workplaces' vulnerabilities which motivate their InfoSec violations. They found that potential perpetrators' perceived liberty and evaluation of the workplace's facilitating conditions (e.g., an overall lax attitude about InfoSec and lack of sophisticated technical protection) could motivate perpetrators' intention to commit the violations (Baskerville, Park & Kim 2014; Kim, Park & Baskerville 2016). Kirlappos, Parkin and Sasse (2014) coined the concept of 'shadow security' to refer to InfoSec workarounds that are unknown to top management and formal InfoSec authority. They further found that these InfoSec workarounds were invented and propagated within departments and via informal InfoSec inductions delivered by employees' direct supervisors.

The recent focus on the impacts of end-users' interactions with their workplace on desirable InfoSec behaviours is evident in recent research. For example, Warkentin, Johnston and

Shropshire (2011) found positive effects of social learning with colleagues on end-users' self-efficacy and InfoSec compliance intention. Humaidi and Balakrishnan (2015) found that transformational and transactional leadership increase perceptions of severity and benefits of InfoSec measures subsequently leading to InfoSec compliance. Kim and Kim (2016) found social pressure can motivate end-users' acquisition of InfoSec knowledge, increasing their intention to comply with InfoSec policy. Recent research has also revisited the impacts of InfoSec-related climates on end-users' InfoSec behaviours. For example, Jaafar and Ajis (2013) and Goo, Yim and Kim (2014) examined end-users' climate perceptions of the observable features of InfoSec environments, which comprise the InfoSec practices performed by colleagues and direct supervisors. Such climate perceptions motivate end-users' actual compliance and compliant intention (Goo, Yim & Kim 2014; Jaafar & Ajis 2013). Similarly, Yazdanmehr and Wang (2016) found an ethical climate can increase end-users' perceptions of norms and InfoSec compliance.

2.2 Refinement of Research Focus

After acquiring an understanding about the key topics and emerging trends in the behavioural InfoSec field, I proceeded to generate potential research ideas for this thesis. The aim of the research was to achieve a balance of practical usefulness and theoretical novelty. To this end, I adopted the problematisation approach (Alvesson & Sandberg 2011).

2.2.1 The Problematisation Approach

Sandberg and Alvesson (2010) argue that gap spotting, or formulating specific research questions by examining an overlooked area, is the most common way to generate research questions. Specifically, Sandberg and Alvesson (2010) identified three versions of gap spotting, namely 1) confusion spotting which aims at finding contradictory evidences, 2) neglect spotting that identifies an area which lacks (good) research and 3) application spotting which seeks shortage of theories or perspectives. While the use of gap spotting can be motivated by the combined effects of institutional conditions, professional norms and the researcher's identity, Sandberg and Alvesson (2010) further argue that the benefit of gap spotting in terms of achieving theoretical novelty is rather limited. They propose the problematisation approach to 'disrupt the reproduction and continuation of an institutionalised line of reasoning' (p. 32) to enable researchers to reach 'new and interesting points of departures for theory development' (p. 33).

The central principles of problematisation focus on familiarising oneself with the common assumptions about the subject to be problematised and then questioning the accepted assumptions of existing theories (Alvesson & Sandberg 2011; Sandberg & Alvesson 2010). However, they caution that researchers should not necessarily deny every assumption to the extent of creating a scientific revolution. On this basis, they explain that there are five types of assumptions that can be problematised by researchers to generate interesting research questions—in-house, root metaphor, paradigm, ideology and field assumptions.

In-house assumptions represent the reasoning accepted as unproblematic by supporters within a school of thought. Alvesson and Sandberg (2011) gave an example of an in-house assumption with the concept of leadership, defined by trait theories as comprising a set of personal features such as knowledge, skills and attitudes. In this case, questioning this assumption means defining leadership by the social context and less by a leader's personal traits. The second type of assumption, root metaphor, refers to the underlying and broad impression of a subject matter. Alvesson and Sandberg (2011) provided an example of a root metaphor assumption which views organisations as a unitary set of cultural values and beliefs held by the organisation members. As such, problematising efforts question the assumption about such unity and uniqueness by bringing in the concepts related to differentiation and ambiguity (Alvesson & Sandberg 2011).

Paradigm assumptions refer to accepted notions at the ontological, epistemological and methodological levels of research focusing on the problematised subject (Alvesson & Sandberg 2011). Ideology assumptions are those that follow political, moral and gender-based beliefs about a subject. Alvesson and Sandberg (2011) highlighted that challenging paradigm assumptions may result in the key ingredient for generating interesting research questions. They gave an example about the dualist ontology that prevalently views professional competence as two separate aspects, namely, a set of the worker's attributes and a set of work activities. On this basis, the researcher challenges this assumption by adopting an interpretive perspective which argues that competence is constructed via lived experience as an inseparable relation between the person and their work. The last type of assumption, field assumption, can be shared across paradigms, schools of thought and disciplines. An example of this assumption is the widely shared belief that humans make rational decisions which can be challenged by forwarding the alternative argument that humans operate within bounded rationality (Alvesson & Sandberg 2011).

2.2.2 Problematising Key Theories in Behavioural InfoSec

I adopted the problematising approach (Alvesson & Sandberg 2011) and reflected on the predominantly adopted theories in the behavioural InfoSec field to identify their assumptions. The predominantly adopted theories (see Section 2.1.4) are the TPB (Ajzen 2011a), PMT (Rogers 1975) and GDT (Straub 1990). These theories are summarised in Table 2.3.

Table 2.3. Predominantly Adopted Theories about Desirable InfoSec Behaviours

Theory	Main factors	Examples
Theory of planned behaviour	• Attitude (towards security policy, security practices) • Subjective norms (from colleagues, direct supervisors, top management) • Perceived behavioural control (self-efficacy, perceived controllability)	Bulgurcu, Cavusoglu and Benbasat (2010a); Herath and Rao (2009a, 2009b); Hu et al. (2012); Ifinedo (2014); Lee and Kozar (2008); Rhee, Kim and Ryu (2009); Safa and Von Solms (2016); Zhang, Reithel and Li (2009)
Protection motivation theory	• Threat appraisal (severity, vulnerability, rewards) • Coping appraisal (response cost, response efficacy, self-efficacy)	Herath and Rao (2009a, 2009b); Lee, Larose and Rifon (2008); Li, Zhang and Sarathy (2010); Mohamed and Ahmad (2012); Siponen, Pahnila and Mahmood (2007); Siponen, Mahmood and Pahnila (2014); Vance, Siponen and Pahnila (2012)
General deterrence theory	• Perceived severity of sanctions • Perceived certainty of receiving sanctions	Bulgurcu, Cavusoglu and Benbasat (2010a); Herath and Rao (2009a, 2009b); Siponen, Pahnila and Mahmood (2007)

2.2.2.1 Theory of planned behaviour

TPB posits that people are inclined to perform a behaviour based on their attitude, dominant subjective norms and perception of their control over the behaviour (Ajzen 2011a). TPB has been widely examined in the context of behavioural InfoSec (Lebek et al. 2014; Sommestad et al. 2014; Warkentin & Mutchler 2014). Sommestad et al. (2014) found that attitude was examined in many studies as the predicted variable and perceived behavioural control and subjective norms were both considered as the best predictors of compliance and misuse (Beta coefficients of 0.25 and above).

2.2.2.2 Protection motivation theory

Similar to TPB, PMT has also been employed in many behavioural InfoSec studies (Lebek et al. 2014; Sommestad et al. 2014; Warkentin & Mutchler 2014). PMT was originally developed to explain peoples' response to fear appeals (Rogers 1975) and the theory was extended by

Rogers in 1983 to understand the effects of persuasive communication on behaviours, especially by focusing on the cognitive processes that mediate behavioural changes (Boer, Seydel & Norman 1996). In addition to behavioural intention as PMT's focal construct, the theory has two main components which are the cognitive evaluations of the threat and the coping solution.

PMT postulates that when people encounter a threat, their evaluation of the threat's severity and their own vulnerability against the threat affect the decision to perform the prescribed coping solution (Rogers 1975). It is expected that the more people perceive the threat's severity and their vulnerability, the more they would think favourably of performing the coping solution. In behavioural InfoSec research, these perceptions are contextualised to account for computer threats such as malware infection and InfoSec incidents (e.g., Dang-Pham & Pittayachawan 2015; Herath & Rao 2009a; Siponen, Mahmood & Pahnila 2014; Vance, Siponen & Pahnila 2012).

The revised version of PMT added the rewards factor which refers to the perceived benefits of not performing the coping solution (Norman, Boer & Seydel 2005). Norman, Boer and Seydel (2005) hypothesised that even though people may recognise the threat's severity and their own vulnerability to the threat, the perceived benefits of performing the risky behaviour can attenuate the other two perceptions. Researchers also contextualised perceived rewards to fit the context of behavioural InfoSec research, such as end-users' perceived convenience of not exercising care when downloading electronic files or not checking whether installed anti-virus software is updated (e.g., Dang-Pham & Pittayachawan 2015; Vance, Siponen & Pahnila 2012).

The second cognitive process evaluates two facets of the coping solution—response efficacy and response cost. Specifically, PMT postulates that people are motivated to adopt the recommended behaviour when they find the behaviour effective for mitigating the threat (Rogers 1975). In contrast, they may feel reluctant to adopt the behaviour if it appears too burdensome or has high response cost. In addition to evaluating the coping solution, PMT hypothesised that people also assess their own ability in completing the recommended task (i.e., self-efficacy) (Rogers 1975). In the context of behavioural InfoSec research, the coping solution appraisal usually refers to the organisation's InfoSec policies or protective measures such as anti-virus software (e.g., Dang-Pham & Pittayachawan 2015; Herath & Rao 2009a; Siponen, Mahmood & Pahnila 2014; Vance, Siponen & Pahnila 2012).

2.2.2.3 General deterrence theory

GDT focuses on employees' perceptions of the facets of organisational sanctions for InfoSec violations—certainty of detection and severity of the sanctions (Straub 1990). According to this theory, potential InfoSec perpetrators feel discouraged from committing InfoSec violations when they perceive that their malicious behaviours can be easily detected and the consequential sanction will be severe (Straub 1990).

GDT has been applied by behavioural InfoSec researchers to predict both compliance and noncompliance (Lebek et al. 2014; Sommestad et al. 2014) and the theory has been further extended by other studies. For example, D'Arcy and Herath (2011) conducted a literature review on the research adopting GDT and proposed investigating additional variables such as virtual status, self-control, self-efficacy and moral beliefs. Guo and Yuan (2012) found that personal and workgroup sanctions, in addition to formal sanctions, impact employees' intention to commit InfoSec violations. Researchers also adopted GDT to explain the motivations of desirable InfoSec behaviours. For example, Bulgurcu, Cavusoglu and Benbasat (2010a) found that employees' perception of sanctions increases perceived cost of noncompliance, increasing their favourable attitude towards compliance. GDT was also combined with PMT (Herath & Rao 2009a) and TPB (Herath & Rao 2009b) to predict employees' intention to comply with InfoSec policies.

2.2.3 Reflecting on the Literature and Generating Research Directions

After reviewing the theories predominantly adopted in the behavioural InfoSec field (i.e., TPB, PMT and GDT) (Lebek et al. 2014; Sommestad et al. 2014; Warkentin & Mutchler 2014), I proceeded to identify these theories' assumptions and problematise them before proposing an alternative perspective and new research directions.

Ajzen (2011a) discusses that TPB has three underlying assumptions. First, the theory assumes that a person's attitude towards a behaviour, perceived behavioural control and perceived social norms all feed into the person's behavioural intention. The second assumption posits that people's behavioural, normative and control beliefs are formed without much cognitive effort and in a biased fashion, because people often receive incomplete information for their decision-making. The third assumption is about the theory's theoretical sufficiency, or whether more predicting variables could be added to the existing model to further explain behavioural intention and actual behaviour. In this regard, Ajzen (2011a) explains that the theory was

explicitly left open for the inclusion of additional variables, but researchers are advised to carefully consider such inclusion.

GDT assumes that potential violators need to be aware of sanctions before feeling discouraged to commit computer abuses (Straub 1990). D'Arcy and Herath (2011) state that GDT has another implicit assumption, that sanctions are perceived the same by all people, yet this assumption was disproved (D'Arcy, Hovav & Galletta 2009; D'Arcy & Hovav 2008). As for PMT, the theory assumes that people recognise an existing fear and evaluate the threat and coping solution before feeling motivated to perform a behaviour (Rogers 1975).

TPB, PMT and GDT were predominantly adopted by behavioural InfoSec research, placing emphasis on the individual's cognitive processes. The theories assume that people would evaluate their personal characteristics and the intended behaviour before arriving at a decision to take actions. Since people operate within their bounded rationality, there is a need to explore contingency variables that determine the decision-making process (Hu et al. 2011). Therefore, one way to contribute to the body of knowledge is by adopting new theoretical frameworks or extending current ones to identify additional variables which impact end-users' InfoSec behaviours.

The assumption focusing on individuals' cognitive processes leads to another common methodological assumption shared among these theories. This methodological assumption treats individual respondents as the main unit of analysis and puts emphasis on these individual respondents' unique characteristics such as perceptions and behaviours. Not only the studies adopting TPB, PMT and GDT follow this methodological assumption, but also those examining theories and frameworks less commonly adopted in the behavioural InfoSec field. For example, social control theory (Hirschi 1969) and rational choice theory (Bulgurcu, Cavusoglu & Benbasat 2010a; Paternoster & Simpson 1996) also focus on the internal cognitive processes which involve individuals' evaluation of their attachment to the social context, or of the advantages and disadvantages associated with the actions to be taken. Similarly, studies about end-users' perceptions of InfoSec policies' characteristics, satisfaction, openness to change, perceived usefulness and other predictors (listed in Table 2.1) (Sommestad et al. 2014) appear to follow this methodological assumption.

With their sole focus on the internal cognitive process and seeing individuals as the main unit of analysis, I contend that prior research has overlooked features of the individuals'

surrounding context which could impact their perceptions and behaviours. In an organisational setting it is reasonable to expect that not every employee has the same level of access to resources and opportunities (Ibarra & Andrews 1993). This presents a situation similar to the concept of bounded rationality where employees develop different perceptions and decide to take actions based on limited information acquired from the sources they interact with.

It is difficult to accurately investigate end-users' various levels of interactions with each other and their access to InfoSec-related resources by following the assumption which emphasises individuals' cognitive processes and by solely collecting data about their perceptions. For example, a person's self-reported perception of their access to a large amount of InfoSec support may not be perceived as equally large by others. Likewise, individuals probably have varied exposure to the sanctions which deter their potential violations, especially in work environments where there are many opportunities to commit violations without being detected. Therefore, researchers cannot derive the characteristics and patterns of the workplace dynamics from such incomparable individuals' perceptions. This limitation obscures the reasons why there are end-users whose InfoSec perceptions and behaviours are more favourably developed or less desirable than others.

In line with the growing research interest in investigating the workplace's impacts on end-users' InfoSec perceptions and behaviours, I propose an alternative perspective that places less emphasis on individuals' characteristics and focuses on the InfoSec-related interactions between these individuals. My proposal presents a paradigm shift in the behavioural InfoSec field which moves researchers from individuals' perspectives to understand what they think and perceive and why they act to a new position where researchers observe individuals as interrelated entities.

To this end, I suggest the adoption of the SNA approach to study phenomena related to end-users' InfoSec perceptions and behaviours. The key feature of a SNA approach is that it treats the network ties, which often represent social interactions and relationships between people, as the main unit of analysis (Borgatti, Everett & Johnson 2013; Hanneman & Riddle 2005; Otte & Rousseau 2002). SNA methods provide the analytical capabilities to investigate the structural patterns of the networks representing people's interactions and to analyse effects of the network ties on individuals' characteristics such as their perceptions or behaviours.

The technical details about the chosen SNA approach and its methods are elaborated on in Chapter 3. The history of the development of SNA and its applications are presented in Section 2.4. The next section discusses the focal theoretical concepts of this research—InfoSec climate and its formation process. The SNA methods provide the analytical capabilities to investigate these concepts with a focus on the social interactions and work environment, in line with the problematisation's outcomes.

2.3 Overview of InfoSec Climate and its Formation Process

The review of current trends in behavioural InfoSec research and the problematisation process suggested pursuing a new research direction which studies the impacts of the work environment on end-users' InfoSec, through investigating via SNA methods the InfoSec-related interactions between these end-users. To this end, I choose to apply SNA methods to investigate the formation of an InfoSec climate or end-users' perceptions of their organisation's shared InfoSec practices (Lowry & Moody 2013). Specifically, these include end-users' perceptions of the InfoSec behaviours performed by their colleagues and direct supervisors (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013).

Despite its importance, InfoSec climate is an under-researched area in the behavioural InfoSec field, as shown by the modest number of studies on the concept (Lebek et al. 2014; Sommestad et al. 2014). InfoSec climate provides a perceptual measure which evaluates the priority of InfoSec in the workplace (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Lowry & Moody 2015) while representing the surfacing manifestation of the more abstract InfoSec culture (Kuenzi & Schminke 2009; Parsons et al. 2015). From the business perspective, evaluating InfoSec climate allows top management to determine whether their employees perceive InfoSec practices as an integral part of their workplace and to devise appropriate strategies for InfoSec management.

2.3.1 Organisational Climate

InfoSec climate is a specific type of organisational climate that comprises employees' shared perceptions of salient organisational features such as policies, practices and procedures that provide cues about expected and rewarded behaviours in the workplace (Schneider, Ehrhart & Macey 2013). Organisational climate was labelled 'one of the fuzziest concepts' (Guion 1973, p. 121) as there were two schools of thought that defined this concept as referring to the

physical and objective attributes of an organisation or the organisation members' psychological perceptions of what they observe at the workplace (James & Jones 1974).

The study of organisational climate originated from the need to investigate how workplaces impact employees' behaviours (Forehand & von Haller 1964). Forehand and von Haller (1964) provided an early definition of the concept as comprising the workplace's stimuli and constraints that are recognised by employees. They proposed five dimensions of organisational climate—organisation's size, structure of authority, organisation's complexity, leadership patterns and goal directions (Forehand & von Haller 1964). Since its inception, the concept of organisational climate has grown in popularity due to its 'undoubtedly important' roles to the 'discovery and development of environmental factors at work that facilitate human well-being and productivity' (Guion 1973, pp. 120–121).

The literature review conducted by James and Jones (1974) identified three approaches to measuring organisational climate: 1) the multiple-organisational attribute, 2) perceptual measurement-organisational attribute and 3) perceptual measurement-individual attribute approaches. Of these, the first approach views organisational climate as being constituted by objective characteristics that distinguish one organisation from another (e.g., size, complexity and leadership style). In contrast, the latter two approaches see the nature of organisational climate as perceptual. They differ from each other; the perceptual measurement-organisational attribute approach regards organisational climate as an attribute of the organisation and focuses on the consensus among the perceivers. The perceptual measurement-individual attribute approach argues that the construct is personalistic and represented by individuals' perceptions of the organisational characteristics that are important to them. James and Jones (1974) referred to the organisational climate conceptualised by the perceptual measurement-individual attribute approach as 'psychological climate' and found that this definition of organisational climate had been receiving more attention than the others.

Schneider and Reichers (1983) considered the categorisation of different approaches to define organisation climate as an advance of climate research. They explained psychological climate as the individual's perceptions of a work context, whereas organisational climate was the people's summated perceptions. By reviewing studies, Schneider and Reichers (1983) noticed that organisational climates for different organisational aspects such as safety, innovation, service, performance and achievement were investigated. Since employees could be involved in thousands of relevant events indiscriminately of relevance at their workplace, they argued

that ‘to speak of organisational climate per se, without attaching a referent is meaningless’ (p. 21). Therefore, Schneider and Reichers (1983) categorised organisational climates into ‘climates for something’ or focused/molecular climates and generic/molar climate. Further, they advised climate researchers to be ‘very clear conceptually about the kinds of climates they wish to assess’ to overcome the generic nature of the climate concept and improve utility of the research through enhanced clarity (Schneider & Reichers 1983, p. 23).

These discussions about the nature and content of organisational climates guided the theoretical definition of InfoSec climate in my research. I examine InfoSec climate as an employee’s perceptions of the important InfoSec practices that reflect the expected and rewarded InfoSec behaviours in the workplace, consistent with Schneider, Ehrhart and Macey’s (2013) definition of organisational climate. This definition is also consistent with those of other behavioural InfoSec studies (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013; Lowry & Moody 2013) discussed in the next section. Moreover, InfoSec climate is recognised as a facet-specific type of organisational climate rather than a generic one. On this basis, its formation process is assumed to follow the forming mechanisms of organisational climates as described elsewhere (Ashforth 1985; Schneider & Reichers 1983).

2.3.2 InfoSec Climate

There are few studies that examine InfoSec climate perceptions. Chan, Woon and Kankanhalli (2005) and Jaafar and Ajis (2013) defined InfoSec climate as employees’ perceptions of the InfoSec state of their organisations, which can be derived from observing the InfoSec practices of top management, direct supervisors and peers. Goo, Yim and Kim (2014) defined InfoSec climate as the perceptual medium that explains the link between the objective characteristics of the workplace and employees’ InfoSec behaviours in the organisation. These definitions of InfoSec climate are similar since they are based on the concept of safety climate, even though Goo, Yim and Kim (2014) disagreed with Chan, Woon and Kankanhalli (2005) and Jaafar and Ajis (2013) in terms of conceptualising and measuring InfoSec climate.

By comparing the similar nature, goals and practices of workplace safety and InfoSec, Chan, Woon and Kankanhalli (2005) adapted the dimensions of safety climate to measure InfoSec climate perception and its components. Specifically, they found employees’ socialisation with colleagues, and their observations of the InfoSec practices performed by top management and direct supervisors, all contribute to the perceived InfoSec climate. The measurement items used

to capture InfoSec climate included the perceived standard of the workplace's InfoSec and how concerned employees believed their top management, direct supervisors and co-workers were about InfoSec. Only Chan, Woon and Kankanhalli (2005) explicitly separated employees' observed workplace features (i.e., their level of socialisation with peers, observed InfoSec practices of top management and direct supervisors) from their climate perceptions (i.e., how concerned they believed their peers, top management and direct supervisors were about InfoSec).

Jaafar and Ajis (2013) examined a theoretical model similar to the model in Chan, Woon and Kankanhalli's (2005) study. However, Jaafar and Ajis (2013) posited employees' perceptions of InfoSec behaviours performed by colleagues, direct supervisors and top management to have direct impacts on employees' InfoSec compliance, rather than having these effects mediated by perceived InfoSec climate as postulated by Chan, Woon and Kankanhalli (2005).

Goo, Yim and Kim (2014) also adapted the dimensions of safety climate to conceptualise InfoSec climate. However, Goo, Yim and Kim (2014) did not separate employees' perceptions of InfoSec behaviours of colleagues, direct supervisors and top management and their perceived InfoSec climate as done by Chan, Woon and Kankanhalli (2005), and did not examine the direct impacts of those perceptions on employees' InfoSec compliance as was done by Jaafar and Ajis (2013). Goo, Yim and Kim (2014) modelled InfoSec climate as a second-order construct which was formed by employees' perceptions of top management's attention to InfoSec, security enforcement, awareness program and policies. Goo, Yim and Kim (2014) did not include socialisation with colleagues as a component of their modelled InfoSec climate construct; InfoSec climate as a second-order construct was examined for its impacts on affective and normative commitments, security avoidance and compliance intention.

2.3.3 The Formation of InfoSec Climate

Schneider and Reichers (1983) identified three perspectives which explain how organisational climates can be formed—structuralist, selection-attraction-attrition and interactionist perspectives. While the structuralist and selection-attraction-attrition perspectives respectively focus on the objective characteristics of the organisation and the arriving of employees with similar attributes at a common workplace that give rise to organisational climates, the interactionist perspective offers a blended explanation for the emergence of organisational climates (Ashforth 1985; Schneider & Reichers 1983). Specifically, the interactionist

perspective posits that perceived climates emerge as a result of employees' efforts to understand the workplace and their roles (Ashforth 1985). The interactionist's explanation of the formation of organisational climates (Ashforth 1985; Schneider & Reichers 1983) was supported by recent climate studies including those that focus on safety climate (e.g., Schneider, Ehrhart & Macey 2013; Zohar 2010) which InfoSec climate was originally modelled after (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014).

The interactionist perspective draws on symbolic interactionism (Sandstrom, Martin & Fine 2014) which explains that meanings are socially constructed by individuals' interactions and negotiations (Ashforth 1985; Weick 1995). On this basis, organisational climates do not differ across workplaces because of their different objective characteristics (as explained by the structuralist perspective) or because of the different compositions of similar members (as explained by the selection-attraction-attrition perspective), but by the unique meanings of the workplaces constructed by the members (Ashforth 1985; Schneider & Reichers 1983). This perspective also explains the learning process used by newcomers to blend into the new environment and contribute to its climate by learning the organisation's logistics, role expectations, tacit norms, power structures, policies and so forth (Ashforth 1985; Morrison 1993). This process, which includes employees' social interactions, observation, reactions and establishment of their social roles in the environment, is referred to as socialisation (Ashforth 1985).

Ashforth (1985) further elaborated on the contributing role of employees' socialisation to the formation of organisational climates by highlighting the roles of informational and normative influences. Employees respond to their constant need to evaluate their skills and beliefs by comparing themselves with colleagues who are similar, valued and accessible. Such comparisons facilitate the social influence which provides information to help individuals understand and predict events in the work environment (i.e., informational influence) which in turn contributes to the development of a shared climate (Ashforth 1985). Conversely, normative influence refers to the social influence that contributes specifically to the institutionalisation of organisational climates by relying on tacit norms and affect (Ashforth 1985).

Studies on InfoSec climate research is scarce (Lebek et al. 2014; Padayachee 2012; Sommestad et al. 2014) with only three studies at present (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013). The conceptualisation or dimensions of InfoSec climate are

not consistent across these studies either. My research will, therefore, measure InfoSec climate on two dimensions—the InfoSec practices performed by an individual's colleagues and their direct supervisors. There are two reasons for this decision. First, these dimensions were included in all three identified InfoSec climate studies (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013). Second, the work practices of colleagues and direct supervisors as salient features of the workplace have been consistently used to measure perception of safety climate (Clarke 2006; Flin et al. 2000, 2006; Guldenmund 2000; O'Connor et al. 2011; Zohar 2014), on which InfoSec climate was modelled. The measurement of InfoSec climate and the theoretical model explaining its formation are discussed in Chapter 6.

2.3.4 InfoSec Climate and InfoSec Culture

The distinction between organisational climate and culture as theoretical constructs was regarded as a confusion and topic of debate (Denison 1996; Moran & Wolkwein 1992). Schneider (1987) argued that climate and culture were complimentary topics, of which the former reflected organisational practices such as reward, support and expectations, while the latter referred to the underlying assumptions and values held by employees. Moran and Wolkwein (1992) described the relationship between climate and culture as two distinctive concepts in detail. Specifically, they defined organisational culture as consisting of three levels ranging from 'creations', i.e., organisational rites and rituals, 'values', i.e., equity and respect for individuals, to the highest level which was 'basic assumptions', i.e., the ideologies and philosophies of the organisation. Organisational climate, as represented by the visible level of supportiveness, achievement orientation or autonomy, operates in between the first and second levels of culture, i.e., 'creations' and 'values' (Moran & Wolkwein 1992).

Moran and Wolkwein's (1992) definition of organisational culture is similar to that provided by Schein's (2010) organisational culture model, which also consists of three levels: (1) artefacts, (2) espoused beliefs and values and (3) underlying assumptions. The artefacts level concerns the visible features of the work environment, including its technology, office layout and behaviour patterns, which can be easily observed but provide little information about the reasons behind group behaviours (Schein 2010). The next level of organisational culture contains espoused beliefs and values, which can be the organisation's strategies, goals and philosophies; the underlying assumptions, as part of the highest level of culture, are the ultimate source of values and actions, including unconscious perceptions, thoughts and feelings (Schein 2010). Moreover, Schein (2010) defined organisational climate as being comprised of the

visible behaviours performed by organisational members, which operates as an artefact of a deeper cultural level.

More recent research focusing on facet-specific organisational climates acknowledged the distinctive features of climate and culture as discussed above (Glisson 2007; Kuenzi & Schminke 2009; Patterson et al. 2005; Schneider et al. 2013; Sopow 2006). For example, Flin et al. (2000) and Zohar (2013) regarded safety climate as the surface measures of safety culture, including the employees' attitudes and perceptions that indicate the values and beliefs about organisational safety. On the other hand, although literature reviews in the behavioural InfoSec field have recognised the existence of studies on InfoSec culture and InfoSec climate (Karlsson, Åström & Karlsson 2015; Padayachee 2012; Sommestad et al. 2014), there is little research to clarify the difference between these concepts. Of these few studies, Parsons et al. (2010) noted that InfoSec climate and InfoSec culture have many overlapping features while citing Schneider's description of climate as being the manifestation of culture that exists at a higher level of abstraction (Schneider 1987).

The concept of InfoSec culture emerged as part of the Third Wave of InfoSec research that focused on the institutional aspects of organisational InfoSec (von Solms 2000). By adapting Schei n's (2010) organisational culture model, behavioural InfoSec researchers have analysed InfoSec culture at three levels, namely artefacts, espoused values and shared tacit assumptions (Alhogail 2015; Furnell & Thomson 2009; Thomson et al. 2006; van Niekerk & von Solms 2010). van Niekerk and von Solms (2010) further proposed InfoSec-related knowledge as a separate fourth level of InfoSec culture thereby highlighting its critical impact on InfoSec culture, rather than including knowledge as part of the other three levels. Additionally, researchers have proposed alternative conceptualisations of InfoSec culture, such as by adapting the organisational culture framework proposed by (Detert, Schroeder & Mauriel 2000). Based on this framework, Chia, Maynard & Ruighaver (2002) and Ruighaver, Maynard & Chang (2007) developed the organisational security culture model which consisted of eight dimensions: (1) the basis of truth and rationality, (2) the nature of time and time horizon, (3) motivation, (4) stability versus change/innovation/personal growth, (5) orientation to work, task, co-workers, (6) isolation versus collaboration/cooperation, (7) control, coordination and responsibility and (8) orientation and focus–internal and/or external.

Ruighaver et al. (2007) discussed in detail each of those eight dimensions of InfoSec culture in their research. In brief, these dimensions, in their order of appearance, refer to: (1) how the

organisation evaluates InfoSec, (2) the short- and long-term InfoSec strategies, (3) employees' motivation to perform InfoSec behaviours, (4) the organisation's tolerance for InfoSec-related changes, (5) InfoSec training and infrastructures, (6) InfoSec governance and collaborative processes, (7) level of InfoSec controls and (8) the organisation's considerations of internal and/or external factors when managing InfoSec. Compared to the three-level conceptualisation of InfoSec culture that follows Schein's (2010) model, Ruighaver et al.'s (2007) organisational security culture model provides a more detailed description of InfoSec culture, which enables a qualitative assessment of InfoSec culture. Further, da Veiga and Eloff (2010) proposed another conceptualisation of InfoSec culture adapted from Schein's (2010) work, and they examined each level of culture at three tiers, namely organisational, group and individual. For instance, they posit that InfoSec-related components and activities at the organisational tier such as strategy, governance and risk management can affect the InfoSec culture's artefacts, values and assumptions at the organisational tier. By examining the three levels of InfoSec culture at three tiers, da Veiga and Eloff (2010) developed a quantitative survey to measure and analyse InfoSec culture.

The literature reviewed in this section suggests that InfoSec climate is as an overlapping part of InfoSec culture. Consistent with Schein's (2010) organisational culture model, InfoSec climate, which is comprised of the observable InfoSec-related socialisation among employees in the workplace (Chan et al. 2005), can be argued to represent the visible artefacts level of InfoSec culture. This InfoSec-related socialisation also reflects several dimensions of InfoSec culture, as defined by Ruighaver et al.'s (2007) organisational security culture model. These are the dimensions of (5) orientation to work, task, co-workers, (6) isolation versus collaboration/cooperation and (7) control, coordination and responsibility. For example, the increased InfoSec-related socialisation would indicate a heightened level of the employees' InfoSec awareness, an organisation's orientation that favours InfoSec collaboration and shared decision making about InfoSec-related matters. With regard to organisational climate's implications in practice, Moran and Wolkwein (1992) discussed that practitioners can make immediate changes in the work environment, e.g., changes in key staff, that quickly affect the organisation's climate but not its culture. Likewise, Denison (1996) argued that organisational climate is temporal and subject to the direct manipulation of influential individuals, whereas culture is rooted in history and sufficiently complex to resist such manipulation. As a result, influencing the InfoSec climate in TTT, through improving the employees' sharing of InfoSec support and stimulating InfoSec-related discussions, and evaluating the changes in the InfoSec

climate are achievable within the short timeframe of this thesis. Provided the close link between organisational climate and culture (Parsons et al. 2010; Schein 2010), improving the InfoSec climate at TTT contributes to shaping a positive InfoSec culture in the future as well.

2.4 Applying SNA Methods to Study Organisational Phenomena

While SNA methods have been adopted in earnest in social sciences (Borgatti & Foster 2003; Otte & Rousseau 2002) adoption has been extremely modest in the behavioural InfoSec field. A search for behavioural InfoSec studies that adopted SNA methods was conducted in scholarly search engines and databases (i.e., Google Scholar, Scopus, IEEE Xplore and ScienceDirect) by using the following keywords:

- 'social network analysis' and 'security behaviour' or 'security behavior'
- 'social network analysis' and 'security perception'
- 'social network analysis' and 'security compliance'

The searches returned only two relevant studies; one was a conceptual research-in-progress (Yoo & Sanders 2013) and the other a Master's thesis which presented the idea of using SNA to diffuse InfoSec awareness (Corona 2008).

2.4.1 The Development of SNA

SNA as a research approach is defined by four key features: 1) the focus on ties that link social actors, 2) the use of systematic empirical data, 3) graphic imagery and 4) mathematical models (Freeman 2004). The history of development of the SNA approach has complicated origins (Scott 2011). *The Development of Social Network Analysis* by Freeman (2004) provides a full and comprehensive chronicle about the development of SNA.

The view of social life as a structure that consists of ties connecting actors has implicitly been recognised for some time. Auguste Comte proposed clearly in 1853 an explicit definition of society as being composed of social interconnections and individuals (Freeman 2004). Various German sociologists in the late nineteenth and early twentieth century embraced Comte's structural perspective. Simmel (1908/2011, p. 23) explained that 'society exists where a number of individuals enter into interactions' which formally established the foundation for SNA (Freeman 2004). In particular, Simmel (1908/2011, pp. 24–25) wrote,

> A collection of human beings does not become a society because each of them has an objectively determined or subjectively impelling life-content. It becomes a society only when the vitality of these contents attains a form of reciprocal influence; only when one individual has an effect, immediate or mediate upon another, is mere spatial aggregation or temporal succession transformed into society. If, therefore, there is to be a science whose subject matter is society and nothing else, it must exclusively investigate these interactions, these kinds and forms of sociation.

Another foundational contribution was the development of the sociometry approach in the 1930s, developed by Moreno, Jennings and Lazarsfeld (Freeman 2004). The sociometry approach introduced the idea of studying social structures as lines and points and in this way specifically aimed at studying organised groups and the position of group members (Moreno 1934). The sociometry approach integrated the four key features of SNA (which had previously been used separately) and further advanced the SNA field (Freeman 2004).

Simultaneously, American researchers Warner and Mayo at Harvard University also investigated network concepts by conducting the famous 'Yankee City' (Warner & Lunt 1941) and bank wiring room studies (Roethlisberger & Dickson 1939). By analysing the systematic data about interactions and visualisation of the networks they found numerous 'clique' structures (Roethlisberger & Dickson 1939; Warner & Lunt 1941). Compared to the sociometry approach (Moreno 1934) the only missing SNA feature from these studies was the mathematical model (Freeman 2004).

Several studies continued to advance key network concepts and shape the modern SNA field. This includes work about social cliques (Luce & Perry 1949), structural balance (Cartwright & Harary 1956) and the applications of graph theory in analysing networks (Frank, Norman & Cartwright 1965). From 1950, there were a number of social network studies (Barnes 1954; Bott 1955; Mitchell 1969) which focused on uniting the separate research traditions and developing a formal methodology for SNA (Scott 2011). The field rapidly expanded in the late 1970s (Scott 2011).

2.4.2 SNA and Organisational Research

The use of SNA methods for investigating organisational phenomena, such as those related to employees' InfoSec perceptions and practices, is of importance to this research. To this end, Tichy, Tushman and Fombrun (1979) proposed a research agenda to use SNA methods to study relationships within and between organisations that would shed light on the changes in organisational structures and individuals' leadership behaviour. Fombrun (1982) suggested that

researchers may employ three strategies to analyse organisational networks: 1) the nodal strategy that studies how individuals' power, innovation, or job satisfaction is affected by their network position, 2) the dyadic strategy that studies quality of relationships or relationship changes and 3) the triadic strategy that studies organisation design and evolution.

Borgatti and Foster (2003) categorised organisational network studies into four types which focus on 1) structural capital, 2) resource access, 3) convergence and 4) contagion (i.e., the creation of shared perceptions by interactions). Structural capital research aims at determining the benefits that an actor or a group receives from their network position or from having a personal network within a specific structure. The resource access type of research seeks to understand actors' success in a network, but puts more emphasis on the flows of resources than on the network typology. Convergence studies rely on the concepts of centrality and structural equivalence to explain the commonalities between similar network environments. Contagion researches aims at explaining how shared perceptions and behaviours are shaped through interactions.

Carpenter, Li and Jiang (2012) proposed another categorisation of organisational network research which covers social capital and network development research at the interpersonal and interorganisational levels. Social capital research focuses on understanding the effects of networks, such as centrality indices and network structures on the individual or organisation, while network development research examines the networks' structural patterns and evolution of network structures. They also posited that for each of these network research types, the networks' characteristics can be studied as a predicted variable or predictor.

In addition to generating theoretical understanding about networks in the organisational context, SNA has been widely applied as part of the interventionists' toolkit to design, facilitate and evaluate change programs (Cross et al. 2006; Cross, Parker & Borgatti 2002; Hatala 2006; Valente et al. 2015). For example, prior studies have applied SNA methods to implement interventions that improved knowledge exchange and information sharing (Cross, Parker & Borgatti 2002; Hatala & Lutta 2009; Parise 2007), developed communities of practice (Cross et al. 2006) and facilitated changes in workplaces' cultural values (Johnson-Cramer, Parise & Cross 2007). This research approach focusing on the use of SNA methods for conducting interventions also resulted in methodological contributions including the strategies (Valente 2012; Valente & Davis 1999; Valente & Pumpuang 2007) and metrics for network interventions (Gesell, Barkin & Valente 2013).

2.4.3 Adopting SNA Methods to Investigate Formation of an InfoSec Climate

My research objective, investigating the formation of InfoSec climate, falls into the contagion or social capital category of network research (Borgatti & Foster 2003; Carpenter, Li & Jiang 2012). Employees' perceptions of an InfoSec climate can be shaped through their socialisation within the workgroup, especially by the normative and informative types of social influence (Ashforth 1985; Chan, Woon & Kankanhalli 2005; Schneider & Reichers 1983). By adopting the network perspective, I can conceptualise employees' socialisation as network ties which transmit social influence from one employee to another. Moreover, the effects of these ties representing social influence on employees' perceptions of InfoSec climate as nodal characteristics can be examined by inferential SNA methods. The SNA approach to design and monitor network-based interventions are especially useful for supporting the collaborating industry partner in my research to achieve their business objective which aimed at improving their organisation's InfoSec environment.

2.5 Chapter Summary

This chapter reviewed the InfoSec research literature, with my research focusing on the dimension that concerns end-users' InfoSec behaviours and perceptions. The literature review presented how this dimension has grown in both importance and complexity to the extent that it emerged into a research subfield called behavioural InfoSec research. The review continued to explore contributions to this field, with many recent studies found to focus on exploring the workplace's impacts on end-users' InfoSec behaviours and perceptions.

Motivated to arrive at a new research direction, I applied the problematisation approach to examine the assumptions of the theories predominantly adopted in the behavioural InfoSec field. I found that the extant behavioural InfoSec literature had focused on individuals' unique cognitive processes and overlooked the interactions between individuals. Consequently, I proposed to adopt SNA methods to investigate such interactions and their impacts on end-users' InfoSec-related characteristics, aligned with recent research focusing on the InfoSec workplace's effects.

Among the concepts related to end-users' InfoSec behaviours and perceptions I chose to investigate the formation of an InfoSec climate. Despite its practical importance, InfoSec climate is an under-researched concept in the behavioural InfoSec field which describes the

priority of InfoSec in a workplace and motivates end-users' InfoSec compliance. Moreover, the formation of an InfoSec climate involves end-users' socialisation as network ties which offers the ideal opportunity to apply SNA methods and examine the unexplored applications of these SNA methods in the behavioural InfoSec field. The remainder of the chapter, therefore, focused on the concept of InfoSec climate, SNA methods and how they fit together.

Chapter 3: Research Design and Methods

This chapter discusses the research design of my thesis. The chapter begins with a description of the selection process for a suitable research approach, identifying action research (AR) as the most suitable approach for this thesis. Next, the characteristics of the AR approach, especially its various forms, are discussed. The canonical action research (CAR) approach was selected because it has important features for achieving both the business and scholarly objectives of this research. The chapter then elaborates on the CAR approach, as well as the strategies and criteria for achieving CAR rigour and concludes by discussing features of SNA as the primary research method of my thesis and providing an overview over my CAR project. The structure of this chapter is summarised in Figure 3.1.

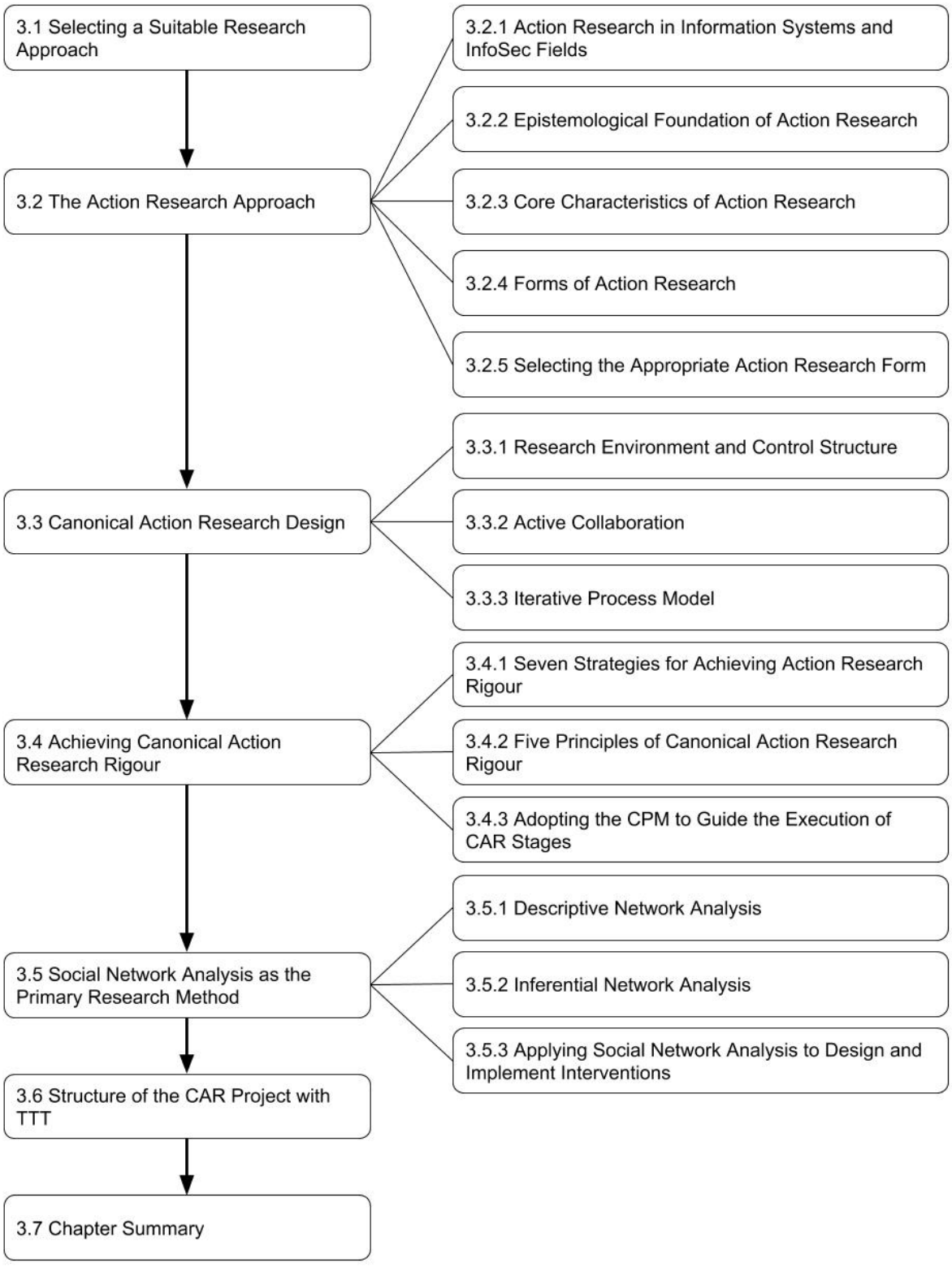


Figure 3.1. Structure of Chapter 3

3.1 Selecting a Suitable Research Approach

There are numerous research designs and methods that a researcher can potentially apply to analyse the formation of an InfoSec climate and to explore the applications of SNA methods in behavioural InfoSec research. One approach to understanding the formation of an InfoSec climate is to identify the factors that impact employees' perceptions of an InfoSec climate either quantitatively or qualitatively. Quantitative techniques such as structural equation modelling (Byrne 2010; Kline 2011) can be employed to evaluate the effects of theoretically grounded factors on an InfoSec climate. This approach is similar to those applied by prior InfoSec climate studies (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013). Identifying the factors that impact the perceptions of an InfoSec climate explains how an InfoSec climate is formed.

Common qualitative approaches to understand the formation of an InfoSec climate include case study or grounded theory approaches. A thoroughly executed explanatory case study based on one or multiple workplaces, where the existence of an InfoSec climate is predominant, can produce lessons learned about the best practices and mechanisms that give rise to an InfoSec climate. The case study approach can be employed to effectively investigate complex social phenomena and result in the development of new theories (Dubé & Paré 2003; Eisenhardt 1989; Gerring 2004). Similarly, researchers adopting a grounded theory approach follow a systematic process of discovering and verifying theoretical concepts from which they can develop a 'thorough theoretical explanation of social phenomena under study' (Corbin & Strauss 1990, p. 5). Such a theory development process can identify the mechanisms, processes and factors related to the formation of an InfoSec climate.

Understanding the formation of an InfoSec climate ideally requires a longitudinal research design which evaluates the changes of the InfoSec climate from one stage to another then determines the factors and mechanisms underlying that forming process. While the mentioned research approaches can be designed as a longitudinal study and accommodate the elements of SNA methods to explore these methods' applications, undertaking any of these approaches will position the researcher away from the studied phenomenon as an external observer—the researcher will barely be able to deeply investigate the formation of the InfoSec climate.

A significant aspect considered for this research was the fact that the approached industry partner, TTT (who granted full access to the company to conduct research), had never

implemented InfoSec improvements before. As a result, there was barely an InfoSec climate in their workplace to examine. The option to seek another organisation with a more mature InfoSec climate was considered, but organisations that had achieved InfoSec maturity may not have detailed memories of the past development of their InfoSec climate. I found an excellent opportunity to collaborate with TTT and enhance their InfoSec climate by using SNA methods, and to explore the formation of an InfoSec climate from the perspective of an insider who monitors that forming process. Performing AR would allow me to be directly involved in the longitudinal transformation of the InfoSec climate at TTT and to understand the critical mechanisms associated with the formation of an InfoSec climate. Therefore, I opted for TTT as collaboration partner and an AR approach as most suitable.

3.2 The Action Research Approach

AR in social psychology originated from the development of action-based research in the 1940s (Baskerville 1999; Baskerville & Myers 2004; Bradbury-Huang 2010; Wallace 1998). After World War II, scientists collaborated with therapists in research projects that developed therapy for social illnesses by intervening in the patient's being or surroundings (Baskerville & Myers 2004). AR focuses on studying complex social processes by introducing changes and observing their effects from which solutions to practical problems and scientific knowledge can be achieved (Baskerville 1999; Baskerville & Myers 2004). Despite previous scepticism of the scientific nature of AR, this research approach has received acceptance in the academic community (Goldkuhl 2012a).

3.2.1 Action Research in Information Systems and InfoSec Fields

AR plays a crucial role in information systems research. Some of its key contributions include the soft systems methodology (Checkland 1988) and the ETHICS approach (Mumford 1995) to information systems development (Avison et al. 1999). Bradbury-Huang (2010) argued that AR has even greater merits than some qualitative methods by conducting research with practitioners rather than about practice, especially since the outcomes concerning practice are 'not something that practitioners can or even wish to make practical use of' (p. 94). Another benefit of the AR approach is the enhancement of competencies and knowledge of all involved stakeholders (i.e., the researchers and practitioners) as a result of the collaborative work (Baskerville 1999). Considering the business objective of TTT to improve their InfoSec

environment and the scholarly motivation for this research, the adoption of an AR approach was expected to produce the most benefits.

AR has previously been adopted by studies in the behavioural InfoSec field and produced important findings. GDT, which explains why employees refrain from violating InfoSec policy as they realise organisational sanctions for InfoSec violations, was an outcome of the AR conducted by Straub (1990). More recent AR in the behavioural InfoSec field includes Puhakainen and Siponen's (2010) research which developed and evaluated an InfoSec training design based on pedagogical theories, and Tsohou et al.'s (2013) study which examined the introduction of InfoSec awareness programs in an organisational context.

3.2.2 Epistemological Foundation of Action Research

AR embraces the notion that knowledge is socially constructed via interventions and interactions with the research participants (Baskerville 1999; Baskerville & Wood-Harper 1998; Coughlan & Coughlan 2002; Wallace 1998). Klein and Myers (1999) argued that different forms of AR may accept the assumptions of various philosophical frameworks.

Baskerville (1999) discussed that AR requires adoption of an interpretivist's perspective during an intervention as the researchers rely on their own observations, personal values and prior knowledge to design and conduct the intervention. Further, Baskerville (1999) recommended that researchers should take into account the social values of the participants and their perceived meanings of the interventions to make the investigation meaningful. This incorporation of the researchers' observations into the design and implementation of the interventions, which subsequently influence the research outcomes, represents the adoption of an interpretive approach in AR (Baskerville 1999).

AR is rooted in pragmatism (Baskerville & Myers 2004; Goldkuhl 2012b; Heikkinen et al. 2012; Jarvinen 2007; Oquist 1978; Reason 2006) due to the core nature of AR which aims to make useful changes in the reality of the participants while contributing new knowledge to theories, corresponding with pragmatism's union of theory and practice. The pragmatist epistemology posits that knowledge arises from human actions while knowing something requires value-directed and purposive change (Oquist 1978). As such, AR requires implementation of problem-based interventions and study of the consequences as knowledge, thus bridging the relationship between knowledge and action (Oquist 1978). Accordingly, I acknowledge pragmatism as the epistemological foundation of AR in this thesis.

3.2.3 Core Characteristics of Action Research

In addition to the discussed benefits, the AR approach has caveats and core characteristics that researchers need to be aware of. Baskerville (1999) noted the four characteristics of AR as 1) aims at understanding an immediate and complex social situation, 2) simultaneously supports problem solving and extends scientific knowledge with the researcher introducing an intervention, 3) is performed collaboratively and improves competencies of all actors and 4) is primarily applicable for understanding change processes in social systems. The involvement of actions and the collaboration with practitioners distinguish AR from other research approaches (Bradbury-Huang 2010).

Goldkuhl (2012a) cautioned that the active engagement with practitioners to jointly solve practical problems in AR may result in consulting work which can jeopardise the goal to generate scientific knowledge. This risk requires researchers to follow certain tenets to avoid such mistake—maintaining a balanced motivation and commitment to both producing scientific knowledge and making practical changes through iterative experiments (Hult & Lennung 1980) and fostering collaboration and deliver theory-based solutions (Baskerville 1999; Baskerville & Myers 2004; Davison, Martinsons & Kock 2004). Solely interviewing or observing the social phenomena without the insights associated with iterative actions does not warrant an AR project (Avison et al. 1999).

My collaborative AR project with TTT to enhance their InfoSec environment posed a challenge as it involved multiple stakeholders—top management, department managers and operational staff across different departments. Further, it was TTT's first experience of implementing an InfoSec change program and top management had great expectations for the program's outcomes. The change program had to be effective, efficient and feasible within the limited resources and time frame of a PhD candidature. These factors indicate the presence of a problem requiring investigation and solution. Further, as a PhD candidate I was motivated by the scholarly goal to produce knowledge addressing the identified theoretical gaps rather than the solely business-orientated objective of solving TTT's InfoSec problem. This demanded a carefully planned approach, reinforcing AR as appropriate for the project.

3.2.4 Forms of Action Research

There are many forms of AR that could be employed for this project. Baskerville and Wood-Harper (1998) identified 10 forms of AR categorised based on four criteria—the type of the

process model, the structure's nature, the researcher's involvement and the primary goals of the AR. These AR forms are summarised in Table 3.1 and are elaborated on to justify the selection of the appropriate approach for this project.

The process models specify how AR should be conducted. The iterative and reflective models follow cyclical processes while the linear model emphasises sequential actions (Baskerville & Wood-Harper 1998). Baskerville and Wood-Harper (1998) argued that the distinction between the first two process models (i.e., the iterative and reflective models) is that the first model focuses more on diagnosing practical problems, whereas the second model aims to discover the differences between the theory followed by the researcher (i.e., the espoused theory) and the theory that emerges from actions (i.e., the theory-in-use). The linear process model puts less emphasis on diagnosing problems and may best be used for solving problems that are clearly identified (Baskerville & Wood-Harper 1998).

The types of structure guide how AR actions should be carried out. In the rigorous structure research actions are executed in an orderly manner which follows a sequential or cyclical process (Baskerville & Wood-Harper 1998). In the fluid structure research actions are loosely defined and performed (Baskerville & Wood-Harper 1998).

Three distinguished forms of researcher involvement indicate the roles of the researcher in an AR project. While collaborative work between the researcher and practitioner is the predominant form, the facilitative and experiment forms set distinctive roles for the researcher and practitioner. The facilitator-researcher is only expected to provide expert advice, while the practitioner is responsible for determining the interventions and vice versa in experimental AR projects (Baskerville & Wood-Harper 1998).

Finally, AR projects must consider their primary goals to select the appropriate AR form that targets their goals. As shown in Table 3.1, goals can be oriented towards organisational development, contributing to system design, prioritising the production of scientific knowledge or simply conducting a training.

Table 3.1. Action Research Forms

	Process model			Structure		Typical involvement			Primary goals			
	Interactive	Reflective	Linear	Rigorous	Fluid	Collaborative	Facilitative	Experiment	Organisational development	System design	Scientific knowledge	Training
Canonical action research	●			●		●			X		X	
Information systems prototyping	●			●		+	+			●		
Soft systems	●				●		●		X	X		
Action science		●			●		●		X		X	
Participant observation		●			●			●			●	
Action learning		●			●			●				●
Multiview			●	●		+	+	+		●		
ETHICS			●	●			●		X	X		
Clinical field work			●		●		●		X		X	
Process consultation			●	●				●	●			

Adopted from Baskerville and Wood-Harper 1998, p. 96.
Key: ● signifies a dominant characteristic, + signifies characteristics that will dominate in different studies, X signifies characteristics that may occur together in the same study.

3.2.5 Selecting the Appropriate Action Research Form

The primary objectives of the AR project in this thesis were producing scientific knowledge about the formation of an InfoSec climate, exploring the application of SNA methods in the behavioural InfoSec field and assisting TTT in improving their InfoSec environment. With these objectives in mind, AR forms which do not prioritise both producing scholarly knowledge and supporting organisational development were identified as inappropriate for this project. These inappropriate AR forms were participant observation and process consultation. Similarly, the information systems prototyping, action learning and multiview forms solely focus on a single objective (i.e., system design or training) while disregarding the goal of producing scientific knowledge. Consequently, these AR forms were considered unsuitable for the AR project with TTT.

Since intervening in employees' InfoSec knowledge and InfoSec climate in the workplace could drastically impact business operations, the top management at TTT preferred making informed decisions after theoretical and pragmatic considerations were thoroughly discussed. I agreed that maintaining a collaborative relationship between the researcher and TTT's top management was prudent and would remove potential bias in planning and executing research actions.

The CAR form, which prioritises fostering a balanced collaboration between the involved stakeholders, satisfied these requirements of the envisioned AR project. The canonical form offered an iterative structure to ensure that the research actions were systematically carried out and it provided researchers with opportunities throughout the iterative cycles to reflect on and refine the actions during the research. Consequently, the canonical form was chosen as the most appropriate AR form for this project.

3.3 Canonical Action Research Design

This research project follows the four core characteristics of CAR: 1) an iterative process model and 2) a rigorous AR structure, which focuses on 3) active collaboration between the researcher and the industry partner (i.e., TTT) with the joint aim to conduct an InfoSec change program contributing to 4) organisational development and the production of scientific knowledge as primary objectives (Baskerville & Wood-Harper 1998; Davison, Martinsons & Kock 2004). In addition to the four characteristics of CAR, a researcher–client agreement (RCA) (alternatively

called client–system infrastructure) is a key component for a CAR project (Baskerville 1999; Davison, Martinsons & Kock 2004).

3.3.1 Research Environment and Control Structure

A RCA is the foundation of any AR project. The RCA outlines the agreed roles of the researcher and the industry partner and establishes the research environment (Baskerville 1999; Davison, Martinsons & Kock 2004). The RCA helps the involved stakeholders set their responsibilities and expectations which subsequently indicate the entry and exit of the researcher and legitimise further research actions if needed (Baskerville 1999).

An RCA for this project, which detailed the responsibilities and anticipated outcomes of the CAR project, was signed by me as the researcher and by the General Director of TTT (see Appendix A). The agreement stated the researcher's intention to anonymously publish the lessons learned from the AR project in the form of scholarly literature and the industry partner's explicit commitment to support the project (Davison, Martinsons & Kock 2004). The agreement confirmed the researcher's and the collaborating partner's acknowledgement of the scholarly objective to generate academic knowledge and the business objective to practically improve the organisational situation. As a result, the agreement prevented conflicts of interest and distinguished the AR project from consulting work (Baskerville 1999; Davison, Martinsons & Kock 2004).

In addition to the RCA, Avison, Baskerville and Myers (2001) recommended considering the three aspects of project initiation, determination of authority and degree of formalisation to maintain AR rigour and ethical actions. An AR project may be initiated by the researcher's need to investigate a theoretical problem and search for a research setting for that purpose (i.e., research-driven) or by the industry partner who confronts a problem that needs to be solved (i.e., problem-driven) (Avison, Baskerville & Myers 2001). This project was originally initiated by my scholarly motivation to investigate the formation of an InfoSec climate and TTT was approached as a host organisation which allowed the investigation. Before my approach and presentation of the research proposal to TTT the objective to enhance the InfoSec environment, albeit deemed later as critical by TTT's top management, was not considered an utmost concern of company or requiring urgent assistance from an external party. Therefore, this AR project's initiation is considered as research-driven.

The authority of an AR project determines the action warrants (i.e., determining the stakeholders who are authorised to execute the interventions) and the processes to negotiate or cancel the AR project (i.e., who are authorised to terminate the project) (Avison, Baskerville & Myers 2001). This authority can be classified into client domination, identity domination and staged domination (Avison, Baskerville & Myers 2001). Client domination does not grant the researcher the authority to implement research actions without the approval of the client. Identity domination refers to AR projects where one or more of the researchers are members of the client's organisation which provides the research team the authority to design and execute research actions.

The authority's pattern of this CAR project is staged domination—power domination flexibly migrates between the researcher and the collaborating industry partner as the project progresses (Avison, Baskerville & Myers 2001). At the beginning of the project I had the authority to propose the appropriate approach for the InfoSec change program that satisfied my scholarly motivation and resulted in the adoption of SNA methods throughout the course of the CAR. As the project progressed to the next stage where specific implementation methods were selected, the industry partner and I had balanced action warrants. To specifically define the power structure of this CAR project, a project team was established to carry out the implementation of the InfoSec change program. The leaders of the project team consisted of the Vice Director of the business solutions provider (BSP) department at TTT and myself as the researcher. Additionally, the General Director was granted the highest authority, including the right to terminate the project upon negotiation with me.

The degree of formalisation of an AR project may be formal, informal or evolved. The first structure requires written agreements which provide descriptions such as problem situation, the scope of the AR project and the team composition (Avison, Baskerville & Myers 2001). Informal control structures for AR do not have written agreements and there may be little shared understanding between the involved stakeholders about the project's scope and issues. In AR projects with an evolved structure there are changes in terms of the project's degree of formalisation as the situation develops. In some cases the formal agreements can also be signed by the researchers and the research clients on the basis of 'do not worry about this it is just formality' (Avison, Baskerville & Myers 2001, p. 36).

Except for the signed RCA and the oral presentations that were conducted in the milestone meetings at the end of stages to report outcomes, most agreements and discussions between

TTT and myself were not formally documented throughout the CAR project. The Vice Director of the BSP department and I, and occasionally top management, discussed the research actions for each stage and kept emails as meeting records which detailed our agreements on the actions. On this basis this CAR project's degree of formalisation was informal or semi-formal.

3.3.2 Active Collaboration

The canonical form of AR prescribes the type of involvement as collaborative—the researcher and the collaborating industry partner make equally important contributions to the AR project (Davison, Martinsons & Kock 2004). In this project, the project team met with top management in the milestone meetings at the end of the stages during which the research outcomes were reported and discussed. The project team also sought support from top management for research actions in these meetings if needed. The decision-making in this CAR project involved myself as the researcher proposing the course of action that would serve both the scholarly and the business agendas. Then the collaborating industry partner and I discussed to reach a consensus on the appropriate actions to be taken and the types of support expected from the industry partner. On this basis we collaboratively shared the responsibility of designing and executing the interventions.

3.3.3 Iterative Process Model

In line with the canonical form this project adopted a five-stage iterative process model (Baskerville 1999; Davison, Martinsons & Kock 2004; Davison, Martinsons & Ou 2012), with the stages of (1) diagnosing, (2) action planning, (3) action taking (intervention), (4) evaluating and (5) specifying learning or reflection. These five stages are illustrated in Figure 3.2.

In a recent development of the CAR iterative process, Davison, Martinsons and Ou (2012) introduced two additional components, the focal and instrumental theories. Focal theories establish the intellectual ground that guides the interventions, while instrumental theories are tools and theoretical models which theorise the intervention's process and how the intervention arrives at its outcomes (Davison, Martinsons & Ou 2012). Davison, Martinsons and Ou (2012) provide examples of focal theories such as TPB (Ajzen 2011b), whereas instrumental theories can be a data model, a business model or a selective coding method of a grounded theory analysis.

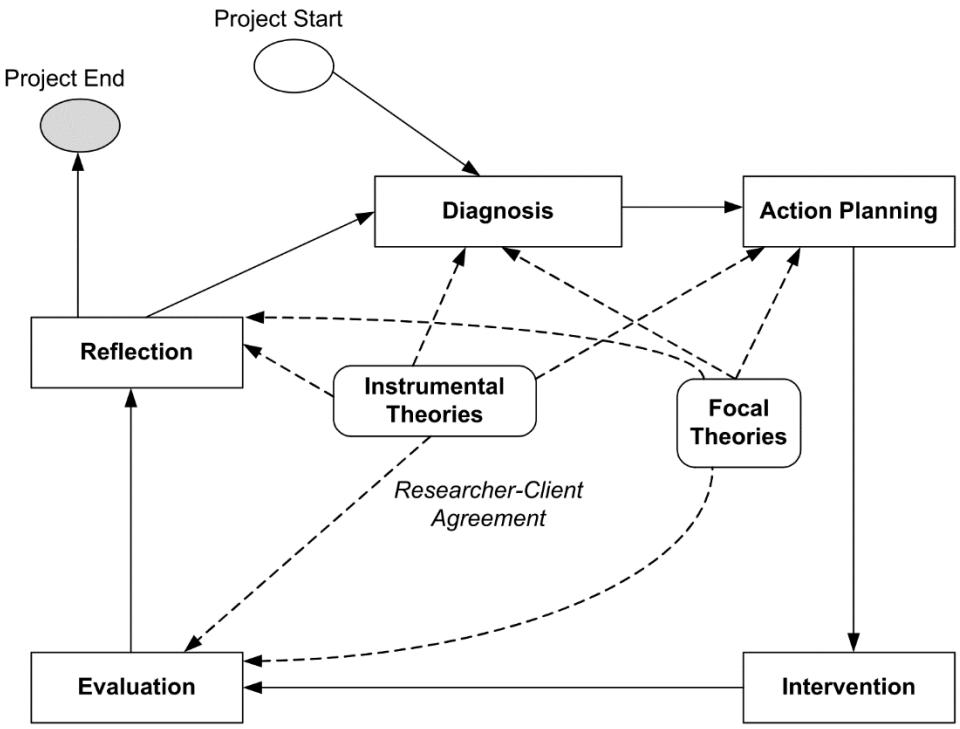


Figure 3.2. CAR Process

Adopted from Davison, Martinsons and Ou (2012, p. 769).
Key: Rectangles represent the CAR process stages. Rounded-corner rectangles represent instrumental and focal theories. Solid lines with arrows indicate the cyclical CAR paths. Dashed lines with arrows represent the links between theories and CAR process stages.

The objective of the diagnosis stage is to clearly understand the situation which involves identifying the nature of the problem and its causes. Moreover, it requires taking into account the outcomes of the research actions performed in the previous iteration. Diagnosing the organisational and research issues is imperative for CAR projects (Davison, Martinsons & Kock 2004), especially for this project since TTT had little InfoSec-related experience and scant knowledge of their InfoSec situation. The initial meeting with TTT's stakeholders to discuss their current InfoSec environment is detailed in Chapter 4. The first stage of this CAR project, described in Chapter 5, was dedicated to diagnosing the InfoSec issues in TTT and understanding the best practices for effective InfoSec implementation in the Vietnamese context. The latter objective was achieved by conducting a case study with InfoSec experts in Vietnam who had successfully implemented the InfoSec standard ISO 27001 in their companies.

The diagnosis stage allows the researcher and industry partner to formulate the intervention in the next action planning stage described in Chapter 6. The research actions should be based on the agreements between the researcher and industry partner (Davison, Martinsons & Kock

2004). During the action planning stage of this CAR project the project team jointly discussed and agreed on the research actions to be performed.

The planned intervention is then carried out in the third stage described in Chapter 7. This taking of action presents the actual intervention. It is recommended that change strategies are employed to assist the intervention, which includes the use of influential agents to diffuse the intended change or to empower individuals and to help them to adopt the change (Baskerville 1999; Davison, Martinsons & Kock 2004). In this CAR project we employed SNA methods to identify influential InfoSec champions who then conducted the change program by diffusing InfoSec knowledge and increasing InfoSec-related socialisation. We also used SNA methods to monitor the effectiveness of the change program.

The intervention's outcomes are evaluated in the fourth stage to determine whether they have met the initial expectations and objectives. Researchers analyse the change process jointly with the industry partner to understand the mechanisms and factors that have resulted in the outcomes (Davison, Martinsons & Kock 2004). The fifth and final stage, reflection or specifying learning, allows the project stakeholders to reflect on the performed actions and the discovered knowledge and, more importantly, decide whether or not the AR project should be concluded (Davison, Martinsons & Kock 2004). It may be necessary to continue the project if the project objectives have not yet been met (Baskerville 1999; Davison, Martinsons & Kock 2004). The evaluation of and reflection on the outcomes of this CAR project are elaborated in Chapter 8.

3.4 Achieving Canonical Action Research Rigour

Rigour in research can be evaluated by examining the research project against various criteria of the adopted research approach. Research rigour generally refers to the methodological soundness and trustworthiness of the findings generated from that approach (Dubé & Paré 2003; Krefting 1991; Thomas & Magilvy 2011). Since this CAR project employed multiple research methods for each stage, including a case study (see Chapter 5) and various SNA methods (see Chapters 6 and 8), the criteria for rigour of each method will be discussed in their respective stage. This section focuses on the components that maintain the overall rigour of the CAR project as a holistic structure which holds the separate methods together.

Several strategies and recommendations exist to achieve rigour of CAR projects. One way of achieving CAR rigour is by closely following the established power structure which covers the three aspects of initiation, authority and formalisation (Avison, Baskerville & Myers 2001) as elaborated in the previous section. Baskerville (1999) presented seven strategies to maintain AR rigour which emphasised careful planning and the adoption of the iterative model and generalising results to similar settings where the theory can be reasonably applied. Similarly, Davison, Martinsons and Kock (2004) argued that CAR rigour has two components, carefully planned and executed research iterations and continuous engagement in problem diagnosis so that the project members can always determine the relevant actions to be taken. Davison, Martinsons and Kock (2004) proposed five principles which serve as a checklist of CAR rigour. These strategies and principles are described in the following sections.

3.4.1 Seven Strategies for Achieving Action Research Rigour

The seven strategies suggested by Baskerville (1999), which focus on the design and implementation of the project, are: 1) consider the paradigm shift, 2) establish a formal research agreement and 3) a theoretical problem statement, 4) plan for data collection, 5) maintain collaboration and learning with the industry partner, 6) encourage iterations and 7) generalise research findings accordingly.

The first strategy highlights the nature of AR which deviates from the traditional positivist philosophy and thus advises researchers to ensure that the research questions can be appropriately answered by conducting AR (Baskerville 1999). The second strategy addresses the use of formal agreements (i.e., RCA) to collect the participants' consent and warrant the researchers' authorities to take actions in the research context (Baskerville 1999). Similarly, the third strategy requires that the theoretical framework guiding the AR project must be documented and explicitly presented, so that the project can be distinguished from consulting work. Baskerville (1999) noted that empirical data in AR projects can be collected in multiple ways such as audio-taped observations, interviews, experiments and cases written by the participants. He further advised researchers to make careful plans for the data collection methods.

The fifth and sixth strategies focus on the process of conducting the AR project. Researchers are advised to avoid assuming a consultant's authoritative role and dominating the planning phases (Baskerville 1999). Moreover, action success and failure should be equally appreciated

and further actions should be taken until the immediate problem is alleviated. Finally, Baskerville (1999) argued that the generated results from the AR project should be generalisable to contexts similar to the immediate research setting or where the outcome can apply.

3.4.2 Five Principles of Canonical Action Research Rigour

Davison, Martinsons and Kock (2004) advised researchers to follow five key principles to achieve CAR rigour—the RCA, the cyclical process model (CPM), a guiding theory, change through action and learning through reflection. These five principles are similar to the seven strategies suggested by Baskerville (1999). For example, Baskerville's (1999) strategies about the research agreement, theoretical problem statement and planned data collection are discussed in Davison, Martinsons and Kock's (2004) first three principles of CAR. Baskerville's fourth and fifth strategies concerning maintaining collaboration with the client and promoting iterative actions are comparable to Davison, Martinsons and Kock's (2004) fourth and fifth principles.

Davison, Martinsons and Kock (2004) offered a checklist of criteria to achieve research rigour which are related to their five principles (summarised in Table 3.2). This CAR project with TTT followed the principles and strategies suggested by Baskerville (1999) and Davison, Martinsons and Kock (2004). While Baskerville's (1999) strategies effectively serve as a holistic framework, Davison, Martinsons and Kock's (2004) checklist was used to evaluate the rigour of this CAR project. This evaluation will be elaborated on in Chapter 9.

Table 3.2. Principles and Criteria of CAR Rigour

Principles	Criteria
Researcher–client agreement	Did both the researcher and the client agree that CAR was the appropriate approach for the organisational situation?
	Was the focus of the research project specified clearly and explicitly?
	Did the client make an explicit commitment to the project?
	Were the roles and responsibilities of the researcher and client organisation members specified explicitly?
	Were project objectives and evaluation measures specified explicitly?
	Were the data collection and analysis methods specified explicitly?
Cyclical process model	Did the project follow the cyclical process model or justify any deviation from it?
	Did the researcher conduct an independent diagnosis of the organisational situation?
	Were the planned actions based explicitly on the results of the diagnosis?
	Were the planned actions implemented and evaluated?
	Did the researcher reflect on the outcomes of the intervention?

	Was this reflection followed by an explicit decision on whether or not to proceed through an additional process cycle?
	Were both the exit of the researcher and the conclusion of the project due to either the project objectives being met or some other clearly articulated justification?
Theory	Were the project activities guided by a theory or set of theories?
	Was the domain of investigation and the specific problem setting, relevant and significant to the interests of the researcher's community of peers as well as the client?
	Was a theoretically-based model used to derive the causes of the observed problem?
	Did the planned intervention follow from this theoretically-based model?
	Was the guiding theory, or any other theory, used to evaluate the outcomes of the intervention?
Change through action	Were both the researcher and the client motivated to improve the situation?
	Were the problem and its hypothesised cause(s) specified as a result of the diagnosis?
	Were the planned actions designed to address the hypothesised cause(s)?
	Did the client approve the planned actions before they were implemented?
	Was the organisation's situation assessed comprehensively both before and after the intervention?
	Were the timing and nature of the actions taken clearly and completely documented?
Learning through reflection	Did the researcher provide progress reports to the client and organisational members?
	Did both the researcher and the client reflect upon the outcomes of the project?
	Were the research activities and outcomes reported clearly and completely?
	Were the results considered in terms of implications for further action in this situation?
	Were the results considered in terms of implications for action to be taken in related research domains?
	Were the results considered in terms of implications for the research community (general knowledge, informing/re-informing theory)?
	Were the results considered in terms of the general applicability of CAR?

Adopted from Davison, Martinsons and Kock (2004).

3.4.3 Adopting the CPM to Guide the Execution of CAR Stages

To further ensure rigour, I employed the CPM to guide the research activities within the five stages of this project, i.e., diagnosis, action planning, action taking, evaluation and reflection. Consequently, each of these stages would have their own diagnosis to assess the current situation, selection of theories to establish the intellectual background underlying the research actions, and the evaluation of and reflect on the outcomes resulting from the actions performed within that stage. Following the steps prescribed by the CPM in each stage would allow me to organise and report these stages in a coherent manner. Moreover, iteratively diagnosing the current situation and reflecting on theories through the stages would enable the project team to

maintain a balanced focus on finding the relevant solutions to the practical problems and on producing scholarly knowledge.

3.5 Social Network Analysis as the Primary Research Method

Based on the premise that AR adopts the interpretive view, Baskerville (1999) argued that qualitative data and methods are typically employed in AR projects. Davison, Martinsons and Kock (2004) extended this view and argued that the triangulation of several methods and types of data is beneficial for CAR projects. Moreover, Davison, Martinsons and Kock (2004) recommend prioritising methods relevant to the immediate context and its problems as this improves the intervention's benefits and ensures that the intervention is properly planned by following a thorough diagnosis.

Following my scholarly motivation and the above recommendations I selected SNA methods as the primary method of enquiry for this CAR project. Specifically, the adoption of SNA enabled me to determine the factors and mechanisms that contributed to the formation of InfoSec climate, thus achieving my scholarly objective. Moreover, these methods allowed me and TTT to identify the InfoSec champions for the InfoSec change program and evaluate the change program's effectiveness with quantitative network measures.

SNA as a research approach puts emphasis on analysing networks—structures made of any interactions or relationships (termed ties or edges) between network actors (termed nodes or vertices). Network actors can be human or non-human. Throughout this CAR project I demonstrated the adoption of SNA to study the network of relationships between InfoSec vulnerabilities, threats and departments (i.e., non-human actors) (discussed in Chapter 5) and the networks representing socialisation between employees at TTT as human actors (discussed in Chapters 6 and 8).

SNA methods enable sophisticated investigations into the network ties which allow the social context of the actors to be analysed in depth (Otte & Rousseau 2002). Therefore, the SNA approach aligns closely with my scholarly motivation of exploring the formation of an InfoSec climate as a function of employees' socialisation, social influence and climate perceptions. SNA methods have been widely used in organisational research (Borgatti & Foster 2003) and recent studies in the information systems field have also employed SNA methods (Kane et al. 2014; Sykes, Venkatesh & Gosain 2009; Zheng et al. 2010). As discussed in Chapter 2,

behavioural InfoSec studies have not yet empirically applied SNA methods and SNA was only referred to by two conceptual studies (Corona 2008; Yoo & Sanders 2013).

Researchers can examine the complete whole network composed of the nodes and their ties or the personal networks of individual nodes (i.e., ego networks) (Borgatti & Foster 2003; Otte & Rousseau 2002). At each level of analysis researchers can use specialised software to compute network measures and use them in several ways. Similar to the traditional research approaches, researchers using SNA methods can also perform descriptive and inferential network analyses.

3.5.1 Descriptive Network Analysis

Researchers describe and analyse networks through their visualisations enabled by software tools or descriptive statistics (Borgatti, Everett & Johnson 2013). Some examples of tools to visualise networks are NetDraw (Borgatti, Everett & Johnson 2002), Gephi (Bastian, Heymann & Jacomy 2009) and Cytoscape (Shannon et al. 2003). Some of these tools include algorithms which visualise the network in different layouts. For example, NetDraw allows grouping the nodes based on their characteristics such as department membership and gender and many visualising tools can assign unique shapes and colours to the nodes based on attributes such as age, seniority, centrality measures and psychometric properties. By analysing network visualisations researchers can identify the key nodes and the distinctive clusters within the network. For example, the widely cited study of Adamic and Glance (2005) demonstrated the use of network visualisation to explore the nature of political blogs, showed as two separate clusters consisting of the right-wing (red) and left-wing (blue) individuals (see Figure 3.3).

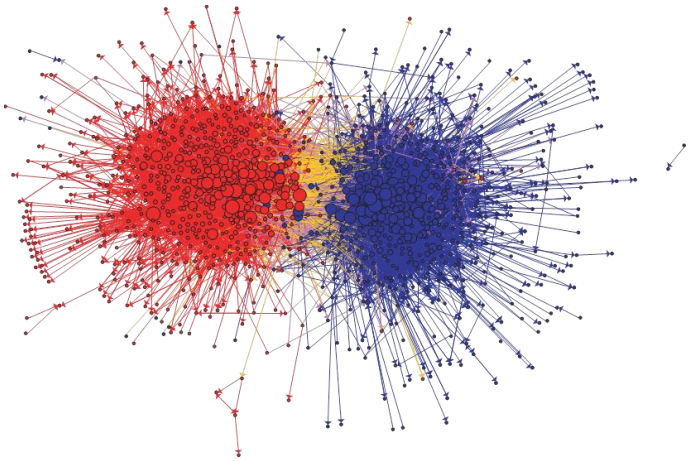


Figure 3.3. Using Network Visualisation to Understand the Like-Minded Nature of Political Bloggers

Adopted from Adamic and Glance (2005, p. 4).

Consistent with the levels of analysis, descriptive network statistics can describe features of the whole network, the nodes in the network and the personal networks of the nodes (i.e., ego networks) (Borgatti, Everett & Johnson 2013). Researchers use descriptive network measures to describe characteristics of the networks such as its density of connected ties or the variations in the numbers of ties possessed by the nodes. The descriptive network measures used in this research are discussed in Chapters 6 and 8.

3.5.2 Inferential Network Analysis

The SNA approach provides several inferential methods for testing hypotheses and statistically evaluating network features. There are two major approaches to test hypotheses with SNA methods. The first involves calculating the network statistics as nodal attributes then using them in regression analyses along with other variables such as demographics, perceptions or behaviours. This approach is especially useful for ego network research where data can be collected from the general population with random sampling techniques (Crossley et al. 2015). Network ties are relational data recorded in an adjacency matrix as illustrated in Figure 3.4. The existence of a tie between a pair of nodes is indicated by a cell in the matrix on the left of the figure, which has a value of '1'. To indicate directions of ties the rows of the matrix denote the senders of ties while the columns denote the receivers. For example, the matrix in Figure 3.4 informs that node 1 sends a tie to node 3, whereas node 3 does not send any ties to node 1.

	Node 1	Node 2	Node 3
Node 1	0	1	1
Node 2	1	0	0
Node 3	0	1	0

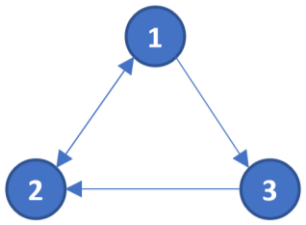


Figure 3.4. Illustration of Relational Data

Testing hypotheses involving network ties requires methods that can appropriately handle relational data indicating these ties. Such relational data violates the independence assumption of standard statistical tests and renders their use inappropriate (Borgatti, Everett & Johnson 2013). This led to the development of specialised inferential analysis methods that are used for testing hypothesis about the occurrence of network ties, such as the quadratic assignment procedure tests, autocorrelation modelling method, exponential random graph modelling (ERGM) method and stochastic actor-oriented modelling method (SAOM).

The simplest method for network hypothesis testing are the quadratic assignment procedure tests available in the UCINET software (Borgatti, Everett & Freeman 2002) and the R package called 'sna' (Butts 2008). Researchers perform quadratic assignment procedure's correlation or multiple regression analysis to evaluate the relationship between multiple types of network ties or predict a type of ties by using other types (Borgatti, Everett & Johnson 2013). Further, individuals' attributes such as gender, age or affiliation can also be converted to the network form and used as variables in these tests. This can be done by creating matrices of matching values (e.g., 1 = same gender, 0 = different gender) or calculating the age differences between pairs of nodes.

Another method to evaluate the likelihood of occurrence of network ties is called ERGM. ERGM offers greater benefits than quadratic assignment procedure's multiple regression analysis as it allows predicting network ties by using a wider range of predictors which include not only ties but also the nodes' attributes and the networks' structural features. For example, researchers employing the ERGM method can test the effects of an employee's age or seniority on the number of interactions or relationships possessed by that employee, or the tendency of two nodes to interact or have a relationship with each other when they have multiple shared partners in between. ERGM can be performed by using the PNet software (Lusher, Koskinen & Robins 2012) or the package 'ergm' in R (Butts et al. 2014).

Researchers may want to focus more on the nodes' attributes rather than the ties between them. In this case, methods such as network autocorrelation modelling (Leenders 2002) and SAOM (Steglich, Snijders & Pearson 2010) can be chosen. For example, Zheng et al. (2010) used the network autocorrelation modelling method to analyse the effects of advice and friendship networks on clinicians' adoption of a healthcare information system together with factors of the technological acceptance model (Venkatesh et al. 2003). A detailed instruction for performing the autocorrelation modelling method is elaborated on by Leenders (2002).

Finally, SAOM is a means to evaluate the changes in both network ties and actor's attributes between several points in time. Performing SAOM is similar to the ERGM method as researchers specify and evaluate a model with terms which describe the mechanisms governing the changes of network ties and attributes over time (Ripley et al. 2017). While both the autocorrelation (Leenders 2002) and SAOM methods (Steglich, Snijders & Pearson 2010) are capable of analysing nodal attributes and are thus suitable for investigating the formation of InfoSec climate, I chose to perform SAOM in this CAR project. The SAOM method allows

not only examination of the changes in nodal attributes, but also the changes in the formation of network ties (Ripley et al. 2017; Steglich, Snijders & Pearson 2010) which are not the autocorrelation method's focus. Therefore, employees' socialisation and social influence—the key mechanisms that lead to climate formation (Ashforth 1985; Chan, Woon & Kankanhalli 2005; Schneider & Reichers 1983)—can be conceptualised as networks and simultaneously analysed with the changing InfoSec climate by using the SAOM method, presenting a complete picture of how an InfoSec climate can be formed.

3.5.3 Applying Social Network Analysis to Design and Implement Interventions

In addition to performing descriptive and inferential analyses researchers also employed SNA methods to design and implement network-based interventions to improve organisational situations (Cross, Borgatti & Parker 2002; Gesell, Barkin & Valente 2013; Hatala & Lutta 2009; Valente 1996; Valente et al. 2015; Valente & Davis 1999). For example, interventionists often used sociometric questionnaires to collect respondents' nominations for interactions or relationships with each other in the same community to detect opinion leaders who can drive the intended change programs (Cross, Borgatti & Parker 2002; Cross, Parker & Borgatti 2002; Valente & Davis 1999). Network-based interventions in the organisational context often aim at improving work collaboration and communication among employees which involve the use of human resource (HR) development practices (Cross et al. 2004; Cross, Borgatti & Parker 2002; Parise 2007; de Toni & Nonino 2010). Moreover, network features such as density, reciprocity, centralisation and transitivity can be evaluated to reflect improvements that result from such interventions (Cross et al. 2004; Gesell, Barkin & Valente 2013; Hatala & Lutta 2009).

Valente (2012) summarised four types of social network-based strategies for designing and implementing interventions—individuals, segmentation, induction and alteration strategies. The first strategy focuses on making use of the opinion leaders, whose network centrality measures are high, to act as change agents which facilitate change programs. The second strategy employs group-detection algorithms to find segments of actors in a network and suitable change programs can be tailored and introduced to each segment. The third strategy creates cascading intervention to be implemented by seed members in the network following snowballing methods. The fourth strategy alters (i.e., creates or removes) network ties and/or nodes for the intervention's purposes.

This CAR project employed the first strategy by using opinion leaders to improve the InfoSec environment at TTT through a diffusion of InfoSec knowledge. The process of using the SNA methods to identify and train champions for the diffusion is discussed in Chapters 6 and 7. The network measures used to evaluate the networks at TTT before and after the diffusion are discussed in Chapters 6 and 8.

3.6 Structure of the CAR Project with TTT

This CAR project adopted the iterative CPM discussed in Section 3.3.3 and illustrated in Figure 3.3. The project started with an initial meeting with the top management at TTT where we established the RCA, formed the project team and determined the project's power structure. In this meeting I also gathered some details of the current InfoSec environment at TTT. This initial meeting is discussed together with a company profile of TTT in Chapter 4.

The diagnosis stage (discussed in Chapter 5) was dedicated to performing a risk assessment which diagnosed the InfoSec environment and issues at TTT. As mentioned earlier, I performed SNA to analyse a network of the InfoSec risks identified from a risk assessment with the department managers at TTT. Moreover, I conducted a descriptive case study with InfoSec experts outside of TTT to understand the critical factors and methods to effectively implement InfoSec improvements in the Vietnamese context. The project team considered this action as necessary as it offered practical considerations for planning and executing the InfoSec change program at TTT.

In the action planning stage (discussed in Chapter 6) I applied SNA to investigate the InfoSec environment at TTT before the change program took place. A descriptive analysis was performed to examine the networks of employees' socialisation. These networks presented employees' provisions of work advice and/or organisational updates, provisions of personal advice and/or trust in colleagues' expertise, provisions of InfoSec advice and troubleshooting support and InfoSec influence. The ERGM method was then employed to determine the factors that enabled employees to exert InfoSec influence over other employees. This led to the identification of the influential InfoSec champions who would carry out the diffusion of InfoSec knowledge as a part of the InfoSec change program. Moreover, the SNA in this stage provided the baseline results which would be compared against the post-intervention outcomes to evaluate the change program's effectiveness.

The action taking stage (see Chapter 7) focused on designing the training materials and delivering the InfoSec training to the selected champions. Key elements for effective InfoSec training and an experiential learning cycle-based InfoSec training approach were used in this stage to guide the research actions. After the training, the champions performed the diffusion of InfoSec knowledge.

In the evaluation and reflection stage (see Chapter 8) I performed SNA to investigate and evaluate the changes in the InfoSec environment after the change program. The SAOM method was employed in this stage to analyse the InfoSec influence network and its impacts on the formation of an InfoSec climate. The project team and top management also evaluated the effectiveness of the change program as reflected by the changes in the InfoSec-related networks. At the end of this stage the project was declared finished when top management and the project team agreed that both the scholarly and business objectives of the project had been met successfully. This meant that the InfoSec environment at TTT had been improved and I had produced scientific knowledge about the formation of an InfoSec climate and about the applications of SNA methods in behavioural InfoSec research.

Overall, the CAR project resulted in three types of research contributions, including organisational improvements, theoretical implications and practical recommendations (Checkland & Holwell 1998). These contributions together with an evaluation of the rigour of the CAR project based on Davison, Martinsons and Kock's (2004) five CAR principles are discussed in Chapter 9. The four stages of this CAR project and its timeline are summarised in Figure 3.5 and Table 3.3 below.

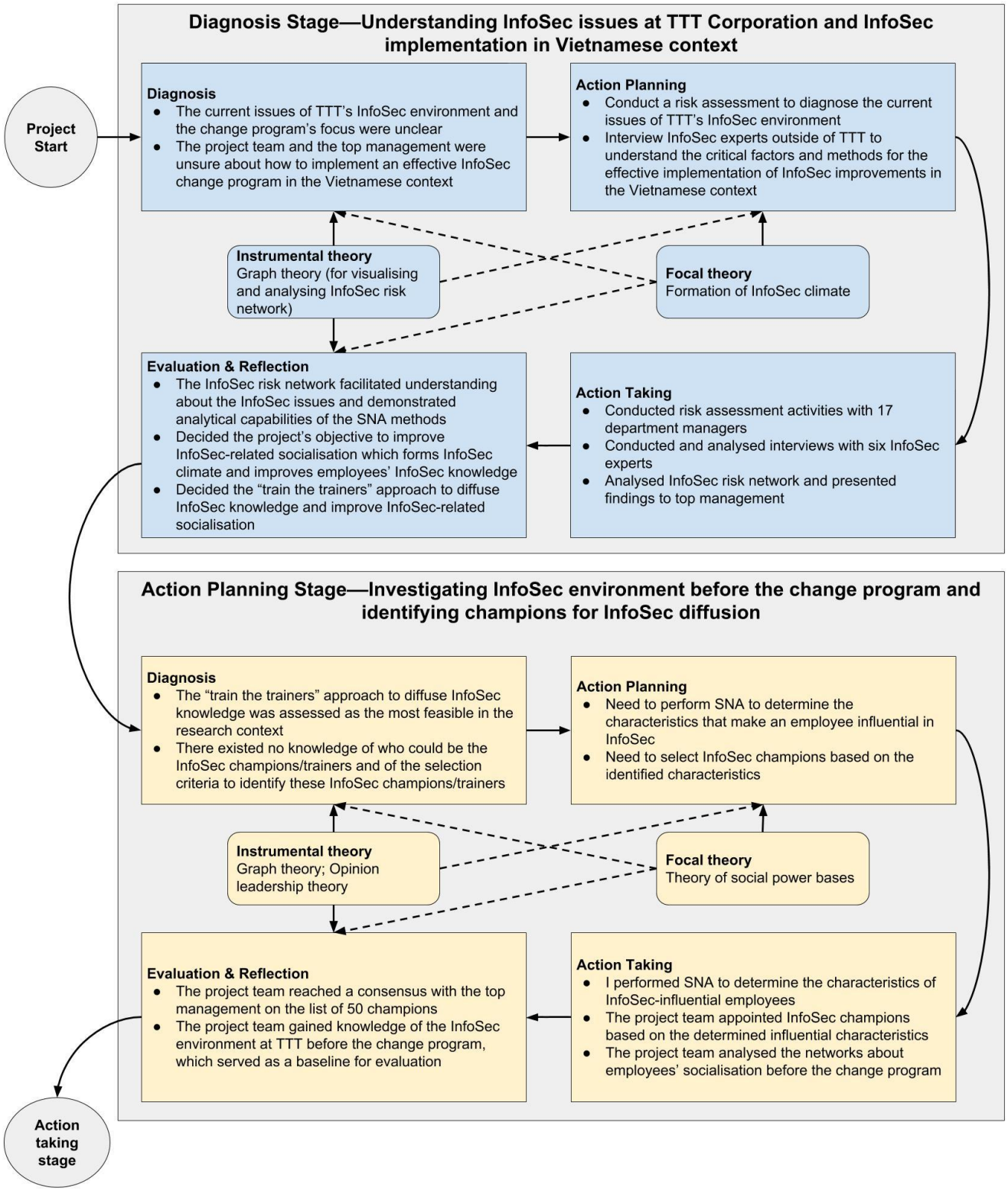


Figure 3.5. Summary of the CAR Project (Diagnosis and Action Planning stages)

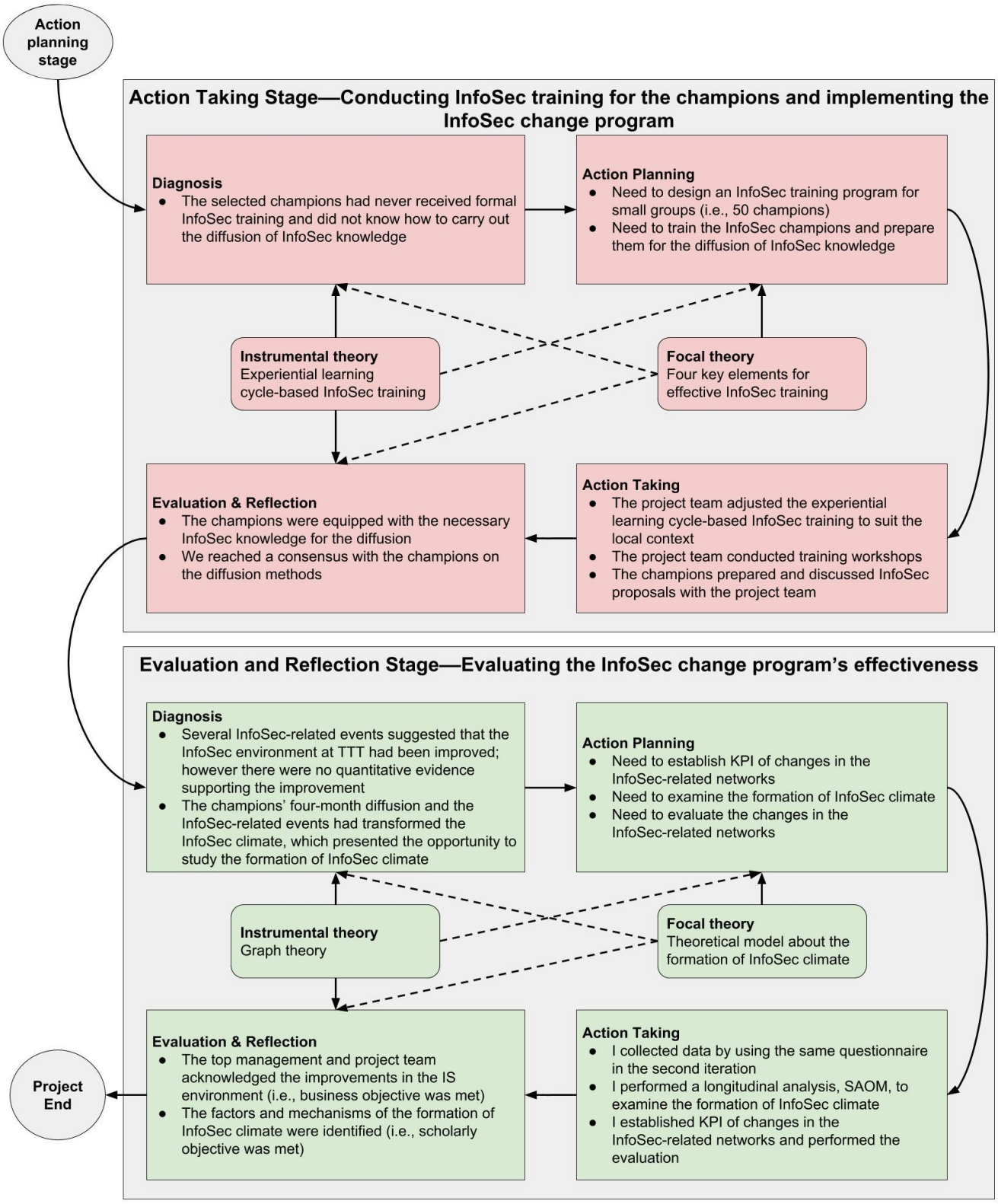


Figure 3.6. Summary of the CAR Project (Action Taking and Evaluation and Reflection Stages)

Table 3.3. Project Timeline

	Date	Research activities
Initial stage	June 2014	I approached TTT's top management for the first time and heard about their business objective to improve InfoSec environment.
	June to 28 November, 2014	I attempted to set up a meeting with TTT's top management. I presented the CAR approach to TTT and explained how this approach could bring benefits to both parties. Top management signed the RCA and allocated the Vice Director of the BSP department to the CAR project.
	December 2014 to February 2015	Vietnam celebrated New Year in December and Lunar New Year in February which lasted for two weeks. TTT was busy with end-of-year operations, and top management advised the project team not to conduct research activities during these periods since the distraction could affect the project's momentum.
Diagnosis Stage	February to April 2015	I reviewed and discussed best practices for implementing InfoSec improvements with the Vice Director of the BSP department.
	April to 17 June, 2015	The project team conducted risk assessment activities, and I conducted the case study with the InfoSec experts at the same time.
	10 July, 2015	The project team presented results from the risk assessment and case study to top management.
Action Planning Stage	July to 4 November, 2015	The project team jointly designed and refined the questionnaire which asked employees about their interactions and perceptions of InfoSec climate.
	5 November to 2 December, 2015	The project team launched the questionnaire for the first time.
	December 2015 to 14 January, 2016	The CAR project was halted due to New Year and Vietnamese Lunar New Year periods again. I presented SNA findings to top management after the Lunar New Year break. We decided the list of InfoSec champions and discussed the next steps for the project.
Action Taking Stage	14 to 24 February, 2016	The project team and top management finalised training materials. The project team conducted the adjusted experiential learning cycle-based InfoSec training for the selected champions.

	24 February to 8 April, 2016	The project team asked the champions to prepare InfoSec proposals which detailed the InfoSec issues in their departments and their proposed solutions. More discussions took place between the project team, top management, and champions to achieve a consensus on the diffusion methods.
	8 April to 8 August, 2016	The champions carried out the diffusion of InfoSec knowledge by conducting InfoSec training or informal discussions with colleagues in the same departments.
Evaluation and Reflection Stage	8 August to 19 September, 2016	The project team launched the questionnaire to collect data about employees' interactions and climate perceptions after the diffusion.
	September to 3 October, 2016	I analysed post-intervention data and presented findings to top management. We agreed that the scholarly and business objectives have been met, and the CAR project was agreed to conclude.

3.7 Chapter Summary

In this chapter the rationale for choosing CAR approach as this thesis' research methodology, to achieve both my scholarly objective to produce scientific knowledge and TTT's business objective to improve their InfoSec environment, was presented. Before deciding to adopt the CAR approach I reviewed other AR approaches and the characteristics of AR in general and found the CAR approach could satisfy the stated objectives. Moreover, I elaborated on the key components of a CAR project such as the roles of the researchers and industry partners, the RCA, the project's authority structure, the five-stage process to conduct a CAR project and the principles to ensure CAR rigour. The chapter also introduced the SNA methods employed as the primary research method throughout this CAR project and concluded with an overview over the CAR project's iterations.

Chapter 4: Canonical Action Research Client's Profile—TTT Corporation

This CAR project took place in TTT, a large interior design and construction enterprise in Vietnam. This chapter provides a descriptive profile of TTT's history and its business, including an explanation of TTT's business needs that contributed to the development of the research questions and partially motivated this research. This chapter further discusses outcomes of the initial meeting between me as the researcher and TTT's key stakeholders (top management and the Vice Director of the BSP department). The structure of this chapter is shown in Figure 4.1.

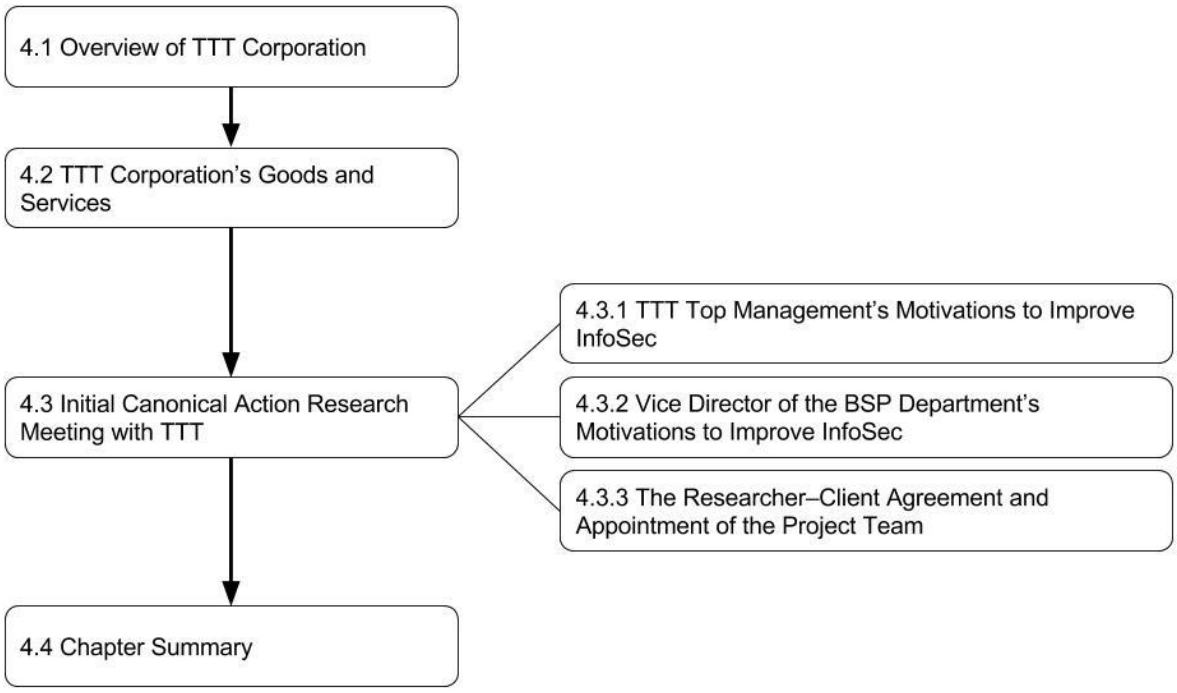


Figure 4.1. Structure of Chapter 4

4.1 Overview of TTT Corporation

TTT was established in 1992 as an interior design and construction company in Vietnam. The organisational chart of TTT is shown in Figure 4.2, where Mr Thong Le Ba is the General Director who oversees the daily operations at TTT.

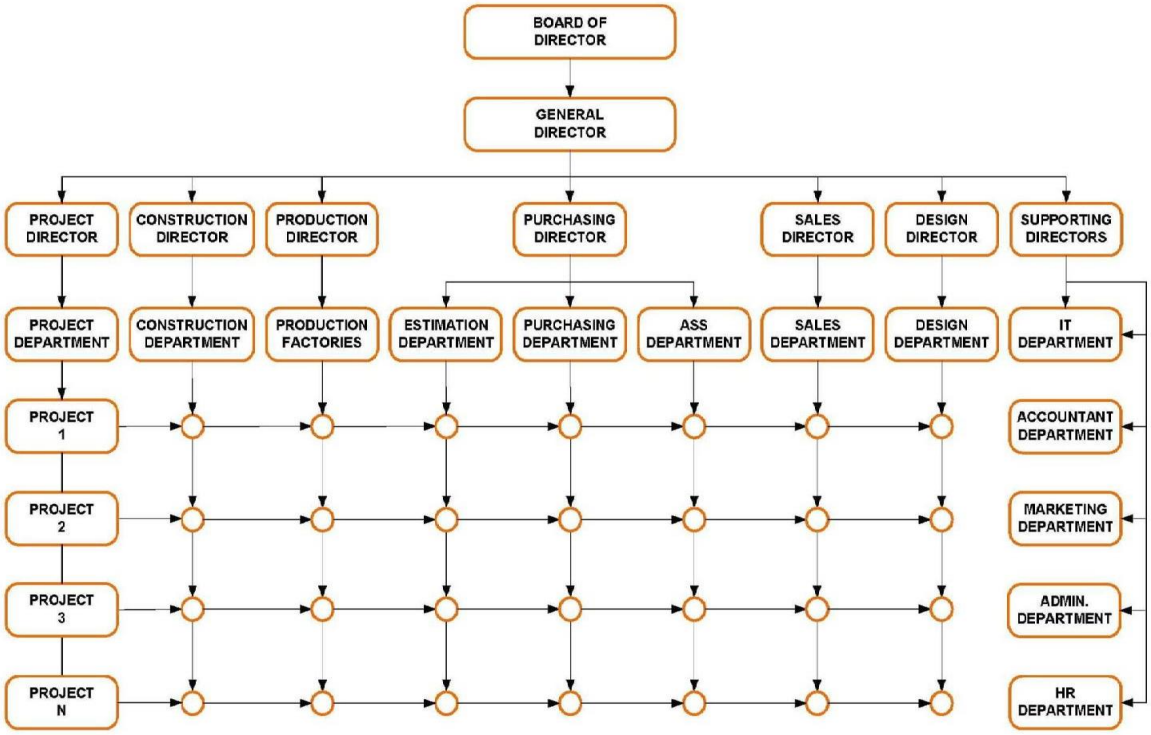


Figure 4.2. Organisational Chart of TTT

Adopted from TTT company brochure.

At the time of the CAR project, TTT employed a workforce of 311 office staff and more than 800 skilled workers. TTT had 20 department (see Table 4.1) of which the project management and construction departments (see Figure 4.3) had the largest number of employees; together with the architect department these departments form the backbone of TTT's business. These project management and construction departments, along with other operational departments such as business development, tender and procurement, are located at TTT's headquarters in Ho Chi Minh City, the most urban city in southern Vietnam.

Table 4.1. List of TTT Office Buildings and Departments

Building	Department (number of employees)	
Headquarters	After Sale Services (7) Administration (15) Business Solutions Provider (5) Board of Directors (9) Human Resource (4) Marketing (2) Purchasing (10) Tender (3)	Accounting (9) Business Development (12) Construction (89) Estimation (7) Information Technology (4) Project Management (29) Quality Control and Assurance (2)
Architect division	Architect (69)	Sourcing (8)
Factory division	Factory (58)	Gamma (sister company) (17)
Ha Noi representative office	Ha Noi Office (7)	

In addition to the project management and construction departments TTT had two departments located in separate office buildings. These were the architect department in a separate office in central Ho Chi Minh City and the factory department in Binh Duong, a suburb on the outskirt of Ho Chi Minh City. A sister company of TTT called Gamma was established in 1999 with an expertise in producing and supplying high-quality office chairs and other furniture. Gamma is located in the same area as TTT's factory department in Binh Duong (see Figure 4.4). There was also a representative office in Ha Noi, the main city in northern Vietnam. Overall, TTT had four offices in Vietnam and was in the process of opening a branch in Myanmar.

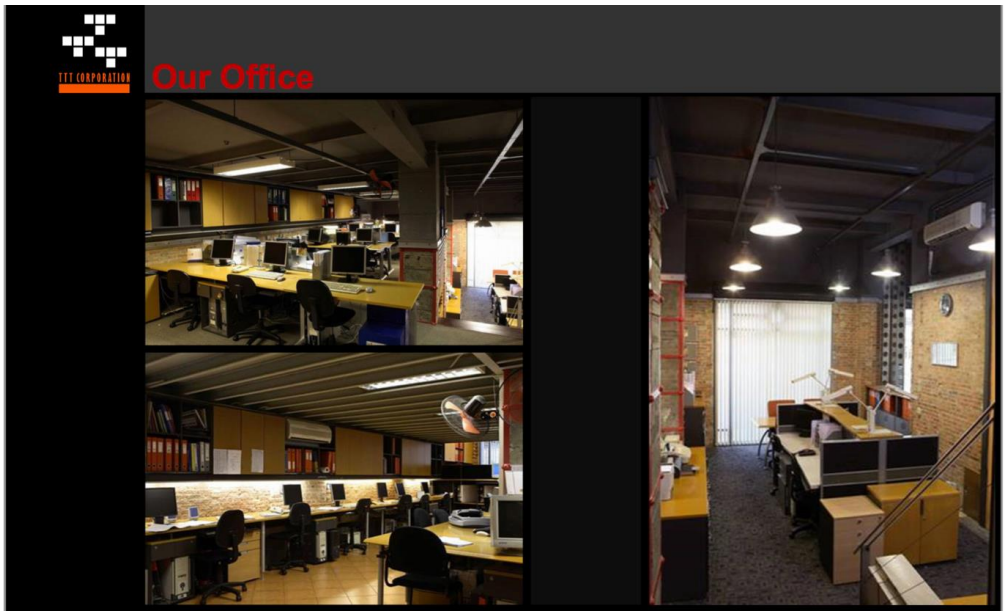


Figure 4.3. The Project Management and Construction Departments in the Headquarter Building

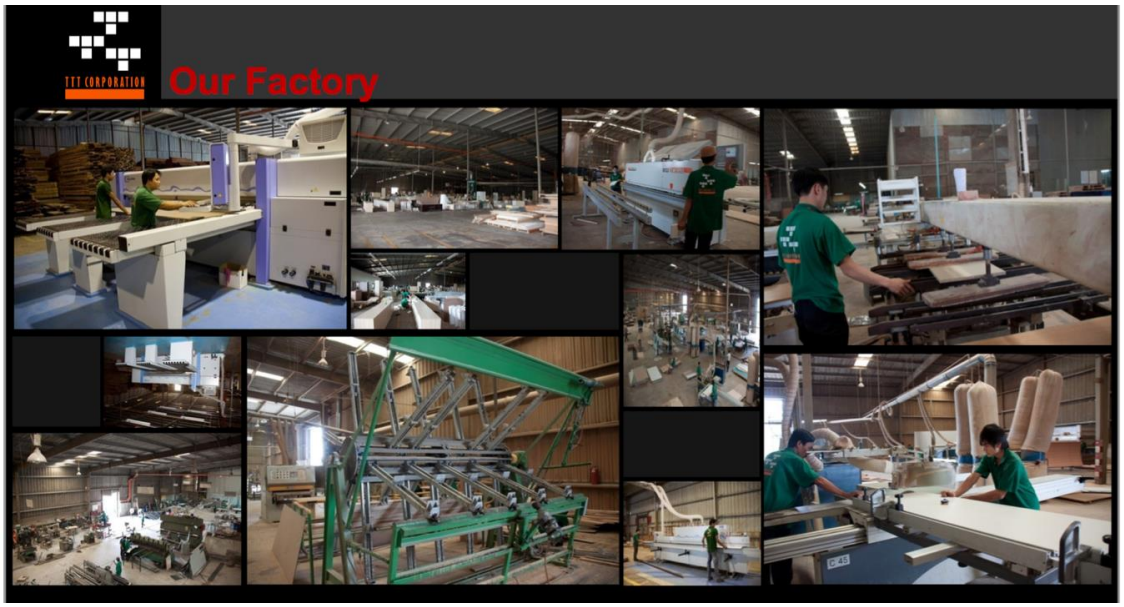


Figure 4.4. The Factory Division in Binh Duong

4.2 TTT Corporation's Goods and Services

TTT identifies itself in the Vietnamese construction industry as the leading design and building contractor specialised in delivering interior design and turn-key construction projects with a focus on office buildings for local and international corporates. TTT attracts 100 to 300 projects annually with primary clients being multinational corporations and local firms. To date, TTT had completed over 1,650 office interior fit-out projects and more than 450 decoration projects for hotels, resorts and serviced apartments.

The architect department itself has completed over 100 architectural designs, more than 1500 interior designs and over 500,000m^2 of office designs. This department had earned TTT many international and national awards including 15 National Architectural Awards, four Ho Chi Minh City Architectural Awards, two international awards and one Vietnam Construction Quality Gold Cup (TCKT 2011; TTT Corporation 2017; Vinh 2015). Additionally, TTT ships furniture manufactured in its factory department and its sister company Gamma worldwide.

4.3 Initial Canonical Action Research Meeting with TTT

To investigate the relationship between an InfoSec climate and dynamics in the workplace, I presented my research proposal and delivered a presentation about my research to large enterprises in Vietnam in need of improving their InfoSec environments. Among the enterprises that responded to my proposal, TTT recognised the alignment between their business objective and my scholarly goals. As a result, an initial meeting was arranged and served to create an understanding between me and TTT's key stakeholders. The following sections explain TTT's motivations to improve their organisational InfoSec and the establishment of the RCA for this CAR project.

4.3.1 TTT Top Management's Motivations to Improve InfoSec

From the initial meeting I understood the reasons that motivated TTT to enhance their InfoSec environment and to enlist academic advice from the researcher. The top management at TTT anticipated that the InfoSec improvements would enhance the company's overall performance by enabling a better customer service level, a more professional brand image and efficient operations while mitigating the existing InfoSec risks in their workplace.

Mr Thong Le Ba, the General Director, and the Director of the HR department were especially interested in making daily operations more ordered and able to accommodate the rapidly increasing amount of information that employees received and processed each day. The confidential and critical information included records of existing and potential clients/suppliers/contractors, bid documents and intellectual property such as furniture designs and architectural blueprints. Further, international and local clients have been demanding organisations in Vietnam to comply with InfoSec and privacy regulations before entering into collaborations. These strategic and operational objectives were the primary reasons that led the top management at TTT to invest resources into enhancing their InfoSec workplace.

4.3.2 Vice Director of the BSP Department's Motivations to Improve InfoSec

The top management had decided in advance that the BSP department under the leadership of its Vice Director would continue to manage and maintain the InfoSec improvements anticipated from this CAR project. Therefore, Mr Tung Doan Van, Vice Director of the BSP department and responsible for the information systems at TTT (e.g., project server, customer relationship management and enterprise resource planning systems), also attended the initial meeting. He described the current technical infrastructure and InfoSec issues at TTT as follows.

According to Tung, most of the computers in TTT were running on the operating systems Windows 7. SharePoint and a project server were deployed to provide a collaborative workspace where employees can monitor projects' progresses and share files with each other. With regard to InfoSec measures, the BSP department and the IT department jointly manage employees' accounts with various access rights allocated to specific roles and departments. A virtual private network, a local area network, a firewall and the WPA2 encryption standard were also in place. To protect the information systems from malicious emails and computer viruses TTT implemented anti-spam and anti-virus solutions. All computers are set up for automatic updates and the company servers are scheduled to perform periodic backups to prevent data loss.

The BSP department also provides employees with a list of approved software that they can download and install on their computers. TTT's employees are required to change their account's password every 42 days and passwords must meet requirements which include 8 characters and a combination of at least one capital letter, one number and one special characters (e.g., @, $ or #). New passwords must not be the same as the last three passwords.

Employee's login account details provide access to three main services at TTT. First, employees can log in to their network account and gain access to the shared file directories of their departments and a common file directory of the whole company named 'TEMP'. Second, this account provides access to an employee's email account. Third, TTT has an intranet web portal where employees can view the company's public announcements and events, training materials and staff list. Employees can create and submit support tickets to the IT department for technical enquiries.

Despite the available InfoSec infrastructure described, Tung displayed concerns about InfoSec threats related to employees' InfoSec knowledge and behaviours. He described threats that stem from employees' undetected use of pirated software and their adoption of mobile devices such as personal laptops, smartphones, tablets, portable drives and personal USBs. All of the attending directors and vice director believed that most of their employees had low InfoSec awareness and knowledge because InfoSec had never been emphasised as a priority by the company or its policies. The consequences of low InfoSec awareness and knowledge were evident in the poor information practices performed by employees in their daily work. As observed by top management these included employees frequently sharing passwords with each other and storing passwords in insecure places, and disorganised work directories and folders on the file server.

Although TTT offered a private cloud system for sharing internal files employees had a habit of sharing files through the 'TEMP' file directory mentioned above. To share the files employees would upload the files to this file directory and recipients would copy the uploaded files to their local machines. This habit posed a critical InfoSec risk as many employees forgot to delete the shared files in the 'TEMP' directory, and sometimes the confidential files remained available to not only the recipients but all TTT employees. In addition to the risk of exposing confidential files to many employees, forgetting to delete the shared files resulted in a disorganised 'TEMP' file directory and consumed a lot of its disk space.

Reflecting on these InfoSec threats, the Vice Director expected that InfoSec improvements would need to focus on enhancing employees' InfoSec knowledge and behaviours. Moreover, he advised that the CAR project should not aim at altering the current technical infrastructure as such modification would require careful planning and potentially significant investment. The General Director also agreed with this advice.

4.3.3 The Researcher–Client Agreement and Appointment of the Project Team

I elaborated on the CAR approach and its principles to the General Director, Vice Director of the BSP department, Director of the HR department and Director of the IT department during the initial meeting, including the importance of establishing a RCA and a formal project team.

A RCA details the mutual understanding between the researcher and the collaborating industry partners about the organisational situation, the boundaries of the problem and the project's objectives, the planned research methods and the commitment and responsibilities of the involved parties (Davison, Martinsons & Kock 2004). Through the RCA the researcher ensures that the clients understand the cyclical approach of CAR and its principles which promote changes through actions and learning through reflection (Davison, Martinsons & Kock 2004).

The Directors of the HR and IT departments, the Vice Director of the BSP department and I decided that the General Director had the highest authority and the right to terminate the CAR project. The General Director agreed to maintain high commitment to the project and provide the necessary support for research activities such as data collection, attending a milestone meeting at the end of each stage and signing off on the project at its conclusion. This project's authority structure was similar to many AR projects in which the external action researchers rarely have the ultimate authority over the project (Avison, Baskerville & Myers 2001).

The General Director, despite having the highest authority to terminate the CAR project if needed, stated that he would not get involved in making decisions related to the specific research actions throughout the project. Such decision-making was to be collaboratively performed by me as the researcher and the Vice Director of the BSP department (co-leaders of the project, hereafter referred to as the project team) to ensure that both the practical needs of TTT and my scholarly objectives would be equally satisfied.

The agreed structure of authority was favourable for me as it afforded the freedom to co-design and co-implement the appropriate research actions with the Vice Director while receiving support from top management. However, TTT's business objective, to enhance the InfoSec environment in TTT, remained unclear at this stage. The project team had to design and implement the necessary actions in the diagnosis stage, which thus focused on diagnosing and understanding clearly the InfoSec issues at TTT, to outline the specific directions for the CAR project.

4.4 Chapter Summary

This chapter introduced the profile of TTT, the industry partner (or research client in CAR terminology) which collaborated with me in this CAR project. The initial meeting with TTT's key stakeholders led to the formation of the project team comprising the Vice Director of the BSP department and myself. TTT believed that there were InfoSec issues in their workplace and the top management recognised the potential benefits from improving TTT's InfoSec environment. Further, they understood the CAR approach and approved the project to commence after the initial meeting. As a result, an RCA which documented the mutual understanding between the researcher and the client with regard to the project's critical components was also prepared. The project team further decided the research actions in the diagnosis stage to focus on diagnosing InfoSec issues at TTT and setting clear directions for the business objective to improve TTT's InfoSec environment.

Chapter 5: Diagnosis Stage—Understanding InfoSec Issues at TTT and InfoSec Implementation in the Vietnamese Context

This chapter discusses the diagnosis stage of the project. The structure and performance of this stage followed the CPM steps suggested by Davison, Martinsons and Kock (2004)—diagnosis, action planning, action taking, evaluation and reflection. Since the project team did not possess up-to-date knowledge of the current InfoSec environment of TTT, this stage was used to perform a full diagnosis of TTT's InfoSec issues. Moreover, it was also necessary to understand the critical factors and methods to implement InfoSec improvements in the Vietnamese context, to develop the change program to improve TTT's InfoSec environment.

Two research actions were performed in this stage to achieve the stated objectives. First, the risk assessment was conducted with the department managers at TTT to understand the current InfoSec issues. Second, a case study was undertaken with six external InfoSec experts to understand the best practices for InfoSec implementation in the Vietnamese context. Each of these research actions had their own action planning, action taking and evaluation stages. The evaluation of these actions' outcomes will be discussed at the end of this chapter. The structure of this chapter is shown in Figure 5.1.

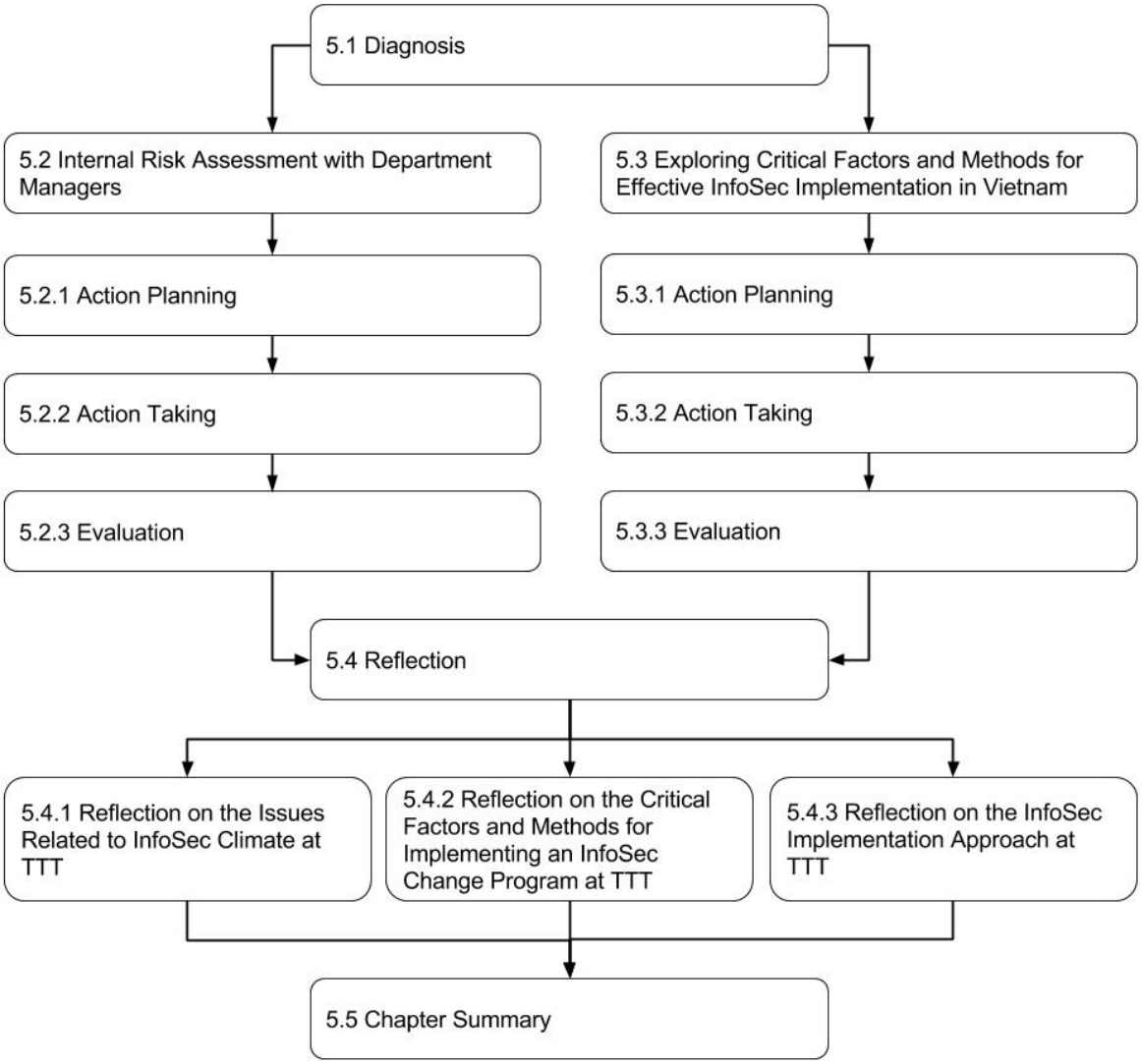


Figure 5.1. Summary of Chapter 5

5.1 Diagnosis

The previous chapter described the profile of the collaborating industry partner and elaborated on the initial meeting that commenced the CAR project. Through the initial meeting the project team made several crucial achievements including gaining top management's support, establishing the project team and acquiring a brief understanding of the current InfoSec environment at TTT. The top management entrusted decision-making to the project team. Despite the technical measures already been in place, the Vice Director of the BSP department proposed to plan a change program focused on improving employees' InfoSec knowledge and behaviours.

A key principle of CAR recommends that researchers consider the research client's opinions when designing the research actions while at the same time conducting an independent diagnosis of the situation (Davison, Martinsons & Kock 2004). Researchers engaged in AR may assume the roles of a resource person who provides expert advice and bring in external resources to jointly solve the identified problems (Baskerville & Wood-Harper 1998; Greenwood & Levin 2007; Park 1999). On this basis, I performed this diagnosis stage to diagnose the critical InfoSec issues at TTT and compared the diagnosed outcome with the opinions of the Vice Director about the InfoSec threats. The outcome of such a risk assessment would provide the directions for designing and implementing an appropriate intervention to improve TTT's InfoSec environment.

An intervention being designed solely based on contributions from the project team and TTT's employees may create biases that could jeopardise the intervention's effectiveness. This motivated me to seek expert insights into the critical factors and best practices for InfoSec implementation in the Vietnamese context. The project team agreed that external expert insights would be useful for accurate planning and design of the intervention and would help minimise erroneous actions, especially since this was TTT's first attempt at implementing an InfoSec-related intervention.

Following the extended CAR principles (Davison, Martinsons & Ou 2012) the project team selected focal and instrumental theories to guide the actions in this stage. The focal theory provides the intellectual basis for the research activities while the instrumental theory directs how these activities are carried out (Davison, Martinsons & Ou 2012). Consistent with my scholarly objective the project team agreed to use the theoretical propositions concerning the formation of InfoSec climate as the focal theory for this stage and the whole CAR project. The adoption of these theoretical propositions offered a systematic approach to analyse the InfoSec environment at TTT by focusing on evaluating the core components of InfoSec climate. Specifically, these components were the observable InfoSec practices performed by employees and their direct supervisors (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013) and the socialisation between employees that facilitates their sense-making activities and contributes to the formation of an InfoSec climate (Ashforth 1985; Dang-Pham, Pittayachawan & Bruno 2015; Schneider & Reichers 1983).

Two CAR research actions were performed in this stage. The three CPM steps for the internal risk assessment with department managers at TTT—action planning, action taking and

evaluation—are discussed in the following sections. Then, the same three CPM steps for the second research action, exploring the critical factors and best practices for InfoSec implementation in Vietnam, will be discussed. Although these research actions were exploratory, they would focus on elements of InfoSec climate such as employees' InfoSec-related socialisation and perceptions as highlighted by the chosen focal theory. Finally, a concluding section is dedicated to present the summarising step of the CPM, namely, specifying learning which reflects on the outcomes of these research actions.

5.2 Internal Risk Assessment with Department Managers

5.2.1 Action Planning

Research on InfoSec implementation has emphasised the importance of involving stakeholders in organisational risk assessment and acquiring their insights into InfoSec issues (Spears 2006). For example, Karyda, Kiountouzis and Kokolakis (2005) specified three important stages for implementing InfoSec policies—the formulation, implementation and adoption stages. Of these, the formulation stage holds a vital role in the implementation of InfoSec policies as it determines the quality of the policies' contents which need to be actionable and relevant to the work context (Karyda, Kiountouzis & Kokolakis 2005). Spears and Barki (2010) employed Markus and Mao's (2004) theoretical framework about information systems users' involvement in the InfoSec context, and found that increased user participation results in greater acceptance of InfoSec measures in the implementation phase. NIST (2011) also highlights the critical role of risk assessment which reveals InfoSec threats and governs the whole implementation of InfoSec improvements. Similarly, the international standard for InfoSec management, ISO 27001, advocates a risk-based approach to implement and monitor InfoSec improvements (ISO 2017). The importance and anticipated benefits of risk assessment activities, as recommended by prior studies and industry standards, justified the performance of a risk assessment in this diagnosis stage.

The project team agreed to use materials of the ISO 27001 standard for the risk assessment activities in this stage. A risk register spreadsheet was retrieved from the 'ISO 27k' website[3], an active professional forum where ISO 27001 experts frequently share resources and advice pertaining to the implementation of ISO 27001 standard. To diagnose the issues related to

[3] http://www.iso27001security.com/index.html (accessed 1 September 2017).

InfoSec climate at TTT while remaining consistent with the scholarly motivation, the project team agreed to use graph theory (Barnes & Harary 1983) as the instrumental theory of this stage.

Graph theory enables the use of SNA concepts to analyse the relationships between InfoSec threats, vulnerabilities and their sources in the form of a network consisting of nodes and ties (Otte & Rousseau 2002; Scott 2012; Wasserman & Faust 1994). Further, researchers can rely on these network-related concepts to calculate quantitative network measures which indicate the importance of the InfoSec threats and vulnerabilities in the risk network. On this basis, the use of SNA methods would practically support the project team to understand the nature of the InfoSec risks while enabling exploration of the applications of SNA methods in a risk assessment.

5.2.2 Action Taking

The project team then jointly designed and performed the risk assessment process as follows. The risk assessment involved the managers from 18 of 20 departments in TTT, excluding the board of directors and a small representative office in Ha Noi that had only eight employees. The project management and construction departments argued that their departments had overlapping confidential files and procedures and, accordingly, they would face similar InfoSec threats. Thus, these departments asked to jointly participate in the risk assessment as one group. This request was approved by the project team.

The department managers first listed the information assets of their department (e.g., customer records, blueprints and databases) and their details, such as the asset's formats (i.e., hard or soft copy), levels of confidentiality, integrity, availability and whether the asset contained personal data or customer data. This step was consistent with the Asset Identification stage in the ISO 27001 risk management framework (ISO 2017). Once all information assets had been documented, the department managers were invited to participate in two brainstorming sessions where they attempted to think of as many InfoSec threats and vulnerabilities in TTT as possible. The completed lists of information assets, threats and vulnerabilities were the prerequisites for the department managers to proceed with completing the risk register spreadsheet.

In the risk register spreadsheet (shown in Figure 5.2) the department managers were asked to assign the three most likely InfoSec threats to each information asset they had identified and

then determine the three most likely vulnerabilities. An additional activity required the department managers to rate the likelihood and impact of the InfoSec threats. On this basis, the spreadsheet automatically calculated the mean risk level for each information asset. The purpose of the risk register spreadsheet was to systematically develop a risk profile for each department which could be revisited and revised in the future.

	A	B	C	D	E	F	G	H
1	ASSET	THREAT (Pick the three most likely threats for the asset)	VULNERABILITY 1	VULNERABILITY 2	VULNERABILITY 3	LIKELIHOOD (1-6)	IMPACT (1-6)	Raw risk level
2	Quality standards document	Internal staff transfer or sell info	Unclear policies about using assets AND sharing info with external parties	No policies about sharing and transferring files across departments	Lack of SETA programs	2	2	4
3		Visitor or family members record audio or take photos of workplace/product/sample	No policies about BYOD/mobile devices usage	Lack of SETA programs		2	2	4
4		Visitor or family members steal or copy info	Unclear policies about using assets AND sharing info with external parties	Lack of SETA programs		2	2	4
5	Quality report	Internal staff transfer or sell info	Unclear policies about using assets AND sharing info with external parties	No policies about sharing and transferring files across departments	Lack of SETA programs	1	3	3
6		Employees verbally leak info to outsiders	No policies about sharing and transferring files across departments	Lack of SETA programs		1	3	3
7		Clients steal and copy info	No policies about sharing and transferring files across departments	Lack of SETA programs		1	3	3

Figure 5.2. Sample Risk Register Spreadsheet

The project team then presented the summarised risk assessment findings to TTT's top management using SNA methods. The relationships between InfoSec vulnerabilities and threats and departments as the sources of these vulnerabilities and threats were conceptually described as 1) the departments have their information assets exposed to one or many InfoSec threats and 2) these threats result from one or many vulnerabilities.

The risk network (see Figure 5.3) visualised the departments (on the right and in dark magenta), the vulnerabilities (at the bottom and in pink) and the InfoSec threats (at the top and in light green). By treating these concepts as connected nodes, I computed their degree centrality, or the sum of ties possessed by a node, to detect centrally important nodes in the network (Borgatti, Everett & Johnson 2013). The sizes of the labels were set as proportional to their degree centrality. A large department node means that the department was exposed to many threats. A large threat node can affect many departments, and a large vulnerability node can result in many threats. The calculation of the nodes' degree centrality was performed by using the SNA software package UCINET version 6 (Borgatti, Everett & Freeman 2002) and the visualisation by using Gephi (Bastian, Heymann & Jacomy 2009).

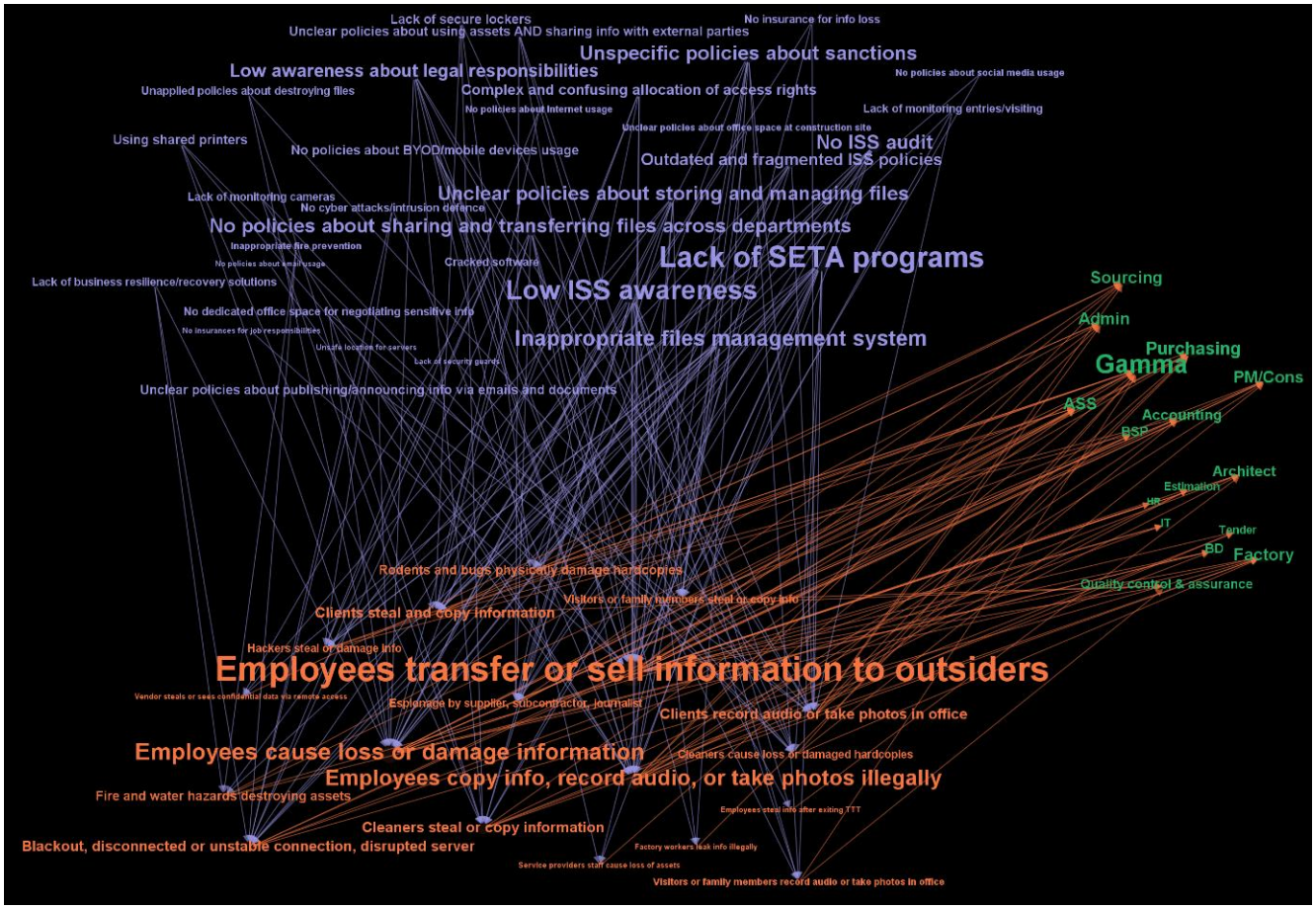


Figure 5.3. Network of InfoSec Risks in TTT

Converting the risk register sheet's data to the relational form of a network enabled me to analyse the similarities between the nodes based on their connections. To this end, I calculated Jaccard coefficients for every pair of the department nodes which denote the percentage of the common ties shared by any two departments (Hanneman & Riddle 2005). A high Jaccard value between two departments indicates that those departments were exposed to similar InfoSec threats. The Jaccard coefficient was the preferred measure to evaluate ties similarity as its calculation only accounts for presenting ties (Hanneman & Riddle 2005), meaning that similarities between the nodes are not inflated by sharing the absence of ties. The analysis of the similarities and dissimilarities of the nodes is discussed in the next section.

5.2.3 Evaluation

Analysing the visualisation of the InfoSec risk network in Figure 5.3 enabled the project team to identify the departments in TTT exposed to the most InfoSec threats and vulnerabilities. Moreover, I calculated the degree centrality measures of the nodes in the InfoSec risk network

which allowed me to rank the nodes based on their importance. These centrality measures and their meanings are presented in Tables 5.1, 5.2 and 5.3.

Table 5.1 presents the vulnerability nodes in the InfoSec risk network and the number of threats which would result from them. The vulnerabilities 'lack of SETA [security education, training and awareness] programs' and 'low ISS [information systems security] awareness' would lead to the highest numbers of threats (13 and 12 threats respectively). Other important vulnerabilities were inappropriate file management system, lack of ISS [information systems security] audit and the lack of or unclear policies about InfoSec procedures. Except for the lack of secure lockers, the identified vulnerabilities were either human- or policy-related. This finding indicated the critical types of vulnerabilities that currently threatened TTT's InfoSec environment.

Table 5.1. Vulnerability Nodes in the InfoSec Risk Network

Vulnerability	Number of resulting threats
Lack of SETA [security education, training and awareness] programs	13
Low ISS [information systems security] awareness	12
Inappropriate files management system	9
No ISS [information systems security] audit	8
No policies about sharing and transferring files across departments	8
Unclear policies about storing and managing files	8
Unspecific policies about sanctions	8
Low awareness about legal responsibilities	7
Outdated and fragmented ISS [information systems security] policies	6
Complex and confusing allocation of access rights	5
Lack of secure lockers	4
No policies about BYOD [Bring Your Own Device]/mobile devices usage	4
Unclear policies about publishing/announcing information via emails and documents	4
Unclear policies about using assets and sharing information with external parties	4
Using shared printers	4
Cracked software	3
Lack of business resilience/recovery solutions	3
Lack of monitoring cameras	3
Lack of monitoring entries/visiting	3
No cyberattacks/intrusion defence	3
No dedicated office space for negotiating sensitive info	3

No insurance for information loss	3
Unapplied policies about destroying files	3
Inappropriate fire prevention	2
No policies about internet usage	2
No policies about social media usage	2
Unclear policies about office space at construction site	2
Lack of security guards	1
No insurances for job responsibilities	1
No policies about email usage	1
Unsafe location for servers	1

Next, the project team analysed the threat nodes and their degree centrality values. The threat nodes, which lay between the vulnerabilities and departments (see Figure 5.3), had their importance measured by two types of degree centrality. First, these nodes had in-degree centrality measures which indicated the number of departments in TTT that these threats could affect. Second, the out-degree centrality reported the number of vulnerabilities that these threat nodes resulted from.

Similar to the previous analysis, the critical threats which were highly ranked based on their degree centrality include those that involve human actors such as employees, cleaners or clients of TTT (see Table 5.2). The department managers felt especially concerned about insider threats caused by employees and cleaners. Additionally, they also considered working with the external clients as risky, given the high numbers of client-related vulnerabilities. This finding suggested that the prevention of these InfoSec threats was not effective. Blackouts and internet disconnection were also deemed important. These issues could disrupt normal business operations (i.e., affect the availability and integrity of the data), but was not considered as a threat to confidentiality of data.

Table 5.2. Threat Nodes in the InfoSec Risk Network

Threat	Number of affected departments	Number of originating vulnerabilities
Employees transfer or sell information to outsiders	16	16
Employees cause loss or damage information	10	15
Employees copy information, record audio, or take photos illegally	9	13
Blackout, disconnected or unstable connection, disrupted server	5	10
Cleaners steal or copy information	5	9

Clients record audio or take photos in the office	5	11
Clients steal and copy information	5	11
Fire and water hazards destroying assets	4	4
Rodents and bugs physically damage hardcopies	4	5
Cleaners cause loss or damage hardcopies	3	7
Espionage by supplier, subcontractor, journalist	3	8
Hackers steal or damage information	3	7
Visitor or family members steal or copy information	3	8
Visitors or family members record audio or take photos in the office	2	5
Employees steal information after exiting TTT	1	2
Factory workers leak info illegally	1	3
Service providers staff cause loss of assets	1	3
Vendor steals or sees confidential data via remote access	1	3

Table 5.3 presents the departments in TTT (excluding the Director Board and the Ha Noi representative office) and the number of InfoSec threats that could affect them. Gamma, as a sister company of TTT, had the highest number of threats, followed by the departments at TTT headquarters that hold key roles in TTT's business.

Table 5.3. Department Nodes in the InfoSec Risk Network and Number of Threats

Building	Department (number of threats)	
Headquarter	Purchasing (7)	After Sale Services (6)
	Administration (6)	Project Management and Construction (6)
	Accounting (5)	Business Development (4)
	Business Solutions Provider (4)	Quality Control and Assurance (4)
	Estimation (3)	Information Technology (3)
	Human Resource (2)	Marketing (2)
	Tender (3)	
Architect division	Sourcing (6)	Architect (5)
Factory division	Factory (6)	Gamma (sister company) (11)

Figure 5.4 summarises the Jaccard coefficients between pairs of departments; green cells show low similarities and yellow and red cells show greater similarities in terms of exposure to the same InfoSec threats.

	ASS	Accounting	Admin	Architect	BD	BSP	Estimation	Gamma	HR	IT	PM/Cons	Purchasing	Quality control & assurance	Factory	Sourcing	Tender
ASS	-															
Accounting	0.22	-														
Admin	0.20	0.57	-													
Architect	0.22	0.43	0.22	-												
BD	0.43	0.29	0.25	0.29	-											
BSP	0.43	0.29	0.11	0.50	0.33	-										
Estimation	0.29	0.33	0.29	0.33	0.40	0.17	-									
Gamma	0.31	0.46	0.55	0.23	0.25	0.25	0.17	-								
HR	0.33	0.40	0.14	0.40	0.50	0.50	0.25	0.18	-							
IT	0.13	0.14	0.29	0.33	0.40	0.40	0.20	0.17	0.25	-						
PM/Cons	0.20	0.38	0.20	0.57	0.25	0.43	0.29	0.42	0.33	0.29	-					
Purchasing	0.44	0.33	0.30	0.20	0.22	0.22	0.11	0.29	0.29	0.11	0.18	-				
Quality control & assurance	0.11	0.29	0.25	0.13	0.14	0.14	0.17	0.36	0.20	0.17	0.25	0.10	-			
Factory	0.33	0.38	0.20	0.57	0.43	0.43	0.50	0.31	0.33	0.29	0.71	0.18	0.11	-		
Sourcing	0.20	0.57	0.50	0.22	0.11	0.11	0.29	0.31	0.14	0.13	0.20	0.30	0.25	0.20	-	
Tender	0.29	0.33	0.29	0.33	0.40	0.17	1.00	0.17	0.25	0.20	0.29	0.11	0.17	0.50	0.29	-

Figure 5.4. Similarities between Departments in Terms of Exposure to InfoSec Threats

The similarities in the departments' exposure to InfoSec threats revealed interesting patterns. For example, pairs of departments such as estimation and tender and project management/construction and factory or architect were found to face many similar InfoSec threats. In contrast, departments such as IT and quality control and assurance did not share similar threats with the other departments. These contrasting patterns suggested that the similar exposure to InfoSec threats was associated with the work relationships between the departments in daily operations which may lead to sharing and co-ownership of information assets. For example, the estimation and tender departments are both in charge of drafting bid documents and costing strategies for the company. The employees in the estimation department were responsible for calculating the estimated costs of a project before the costs were transferred to the tender department's employees to review and to prepare the documents and strategies for project bidding. Likewise, the departments of project management/construction, architect and factory work closely with each other in projects. The collaboration between the project management/construction and the factory departments is especially more intense as employees of the factory department need to ensure the timely supply of high-quality furniture and any necessary replacements upon a project's demands. On the other hand, employees in the IT department rarely get involved in these departments' operations. Due to the intensive collaboration which involves frequent communication and circulation of information assets, departments would face similar InfoSec threats and confidential information might be leaked in the collaborative processes.

During the risk assessment process, the project team also exchanged qualitative feedback with the department managers. Most department managers confirmed top management's belief that

InfoSec had not been receiving attention from many employees. Some managers confessed to vaguely understand that InfoSec issues were related to the infection of computer viruses from malicious websites and emails that could affect the company's information systems somehow. The BSP department had installed anti-virus software on the company's computers and recommended all employees to occasionally check for the software's updating status. However, the department managers commented that most of their employees neither knew how to perform such actions nor had the habit of performing this InfoSec practice. The department managers further reported several InfoSec incidents caused by employees, including forgetting printed documents in the printing area and carelessly disclosing bid profiles and costing strategies to external clients. While the latter type of incidents would pose a substantial risk to TTT, the department managers believed that it was mainly due to employees failing to recognise the confidentiality of the information that they shared with the clients which led to unintentional leakage.

A positive InfoSec climate is reflected by the InfoSec practices actively performed by colleagues and direct supervisors and the socialisation about InfoSec matters between employees (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013). The reported InfoSec incidents and employees' poor InfoSec awareness in general suggested that an InfoSec climate was lacking at TTT. Moreover, the project team also found there were no proper communication and training programs to alleviate the problem. The highlighted human-related InfoSec issues in the InfoSec risk network motivated our intention to design and implement a change program that focused on improving employees' InfoSec knowledge. TTT top management, after reviewing the risk assessment findings, agreed with this intention.

Finally, the project team observed positive reactions from the department managers during their participation in the risk assessment activities. The discussions with the managers were lively and they contributed thoughtful insights into their departments' information assets, threats and vulnerabilities. Some managers admitted that they were glad to see the company had finally invested considerable effort into conducting a formal project to address the InfoSec issues. The buy-in gained from the top management and department managers established a solid foundation for the next CAR activities.

5.3 Exploring Critical Factors and Methods for Effective InfoSec Implementation in Vietnam

5.3.1 Action Planning

In addition to diagnosing TTT's InfoSec environment, the project team agreed that the researcher would consult external experts to understand the critical factors and best practices for effective implementation of InfoSec improvements in Vietnam. The knowledge of these critical factors and best practices was anticipated to guide the change program at TTT and minimise erroneous actions. The task to determine the critical factors and best practices for InfoSec implementation in the Vietnamese context was exploratory in nature. This called for the adoption of a case study approach which involved interviewing InfoSec experts in Vietnam and conducting thematic analysis to identify the success factors of InfoSec implementation. Case study as a research method is 'an empirical enquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident' (Yin 2009, p. 13). The implementation of InfoSec involves both complexity (Merete, Albrechtsen & Hovden 2008) and is also contextual as it concerns various organisational and cultural factors (Crossler et al. 2013; Saint-Germain 2005). Further, the project team decided to interview InfoSec experts who had experience implementing the international InfoSec standard ISO 27001 to ensure these experts had practical knowledge that could be considered when designing the change program at TTT.

The rigour of case study research is evaluated based on multiple criteria in each stage of conducting the study. The first criterion is to clearly define a research question and the case study's design (Dubé & Paré 2003; Riege 2003). With regard to the research question, this diagnosis stage aimed at identifying the critical factors of InfoSec implementation in the Vietnamese context by interviewing ISO 27001 InfoSec experts.

Describing the unit of analysis in case study research is challenging as there are various terminologies used to define a case study and its components. In this matter, Gerring's (2004) definitions of case study elements are quite concise. Gerring (2004, p. 342) explained a case study as 'an intensive study of a single unit for the purpose of understanding a larger class of (similar) units'. A unit represents a phenomenon which comprises a sample of cases and each case comprises several variables (Gerring 2004). Based on this terminology, the phenomenon or unit of interest for the case study embedded in this CAR project was the implementation of

ISO 27001 standard in the Vietnamese context, from the perspectives of the InfoSec experts as studied cases. The objective was to explore the critical factors of ISO 27001 implementation which were the variables of the case study. The case study of this stage belonged to the category of a single-unit case study suitable for focusing on the depth of the phenomenon via internal comparisons (Gerring 2004).

5.3.2 Action Taking

Dubé and Paré (2003) further recommend a criterion for case study's rigour which is to clearly explain the data collection process. Over a period of one month, invitations were sent to InfoSec experts in charge of ISO 27001 implementation projects in their firms in Vietnam. I approached InfoSec experts via online social platforms and forums for professionals including LinkedIn and Facebook's community pages of Vietnamese IT experts and through personal contacts and referrals.

Of the seven InfoSec experts who agreed to be interviewed, one expert from a multinational hardware manufacturing corporation refused to participate after consulting with their external affairs department. Overall, most of the invited experts displayed concerns about answering topics related to organisational InfoSec even though ethics clearance (see Appendix B) and measures to protect the participants' anonymity had been explicitly demonstrated. These concerns were consistent with Kotulic and Clark's (2004) discussion on the intrusive nature of InfoSec research that commonly results in a low response rate from industry stakeholders.

Semi-structured audio-recorded interviews in Vietnamese were conducted in person and online with six InfoSec experts (see Table 5.4). The interview questions (see Appendix C) were designed by myself and two academics in the information systems field following the responsive interview's format suggested by Rubin and Rubin (2011). The interviews lasted for an average of one hour and brief analysis was performed after every interview to add or modify the questions for the next interview.

Table 5.4. Backgrounds of Interviewed InfoSec Experts

ID	Occupation	InfoSec-related experience	Industry
EX1	Consultant/IT Auditor	3 years	Banking and financial services
EX2	IT Manager	14 years	IT services
EX3	Consultant	5 years	Banking
EX4	Information Security Officer	7 years	IT services

EX5	Deputy IT Director	10 years	Banking
EX6	Data Security Manager	3.5 years	Engineering and electronics

I transcribed the interviews myself and used the qualitative analysis software NVivo 11 to analyse the transcripts. Within-case and cross-case analyses were performed to search for major themes to support internal validity (Dubé & Paré 2003; Riege 2003). The analysis process was as follows. When I was conducting the interviews, I took note of the concepts that appeared critical for InfoSec implementation. Next, I briefly reviewed the notes after each interview to determine whether the critical factors identified from the previous interview appeared again in the current one and, where necessary, asked the interviewees additional questions for further elaboration. I analysed then each case (i.e., the interview with each InfoSec expert) separately and coded the critical factors for InfoSec implementation in NVivo. The findings were compared across cases and I identified the consensus and divergences from the cross-case analysis. Finally, validity was achieved by having the informants review the case study report (Dubé & Paré 2003; Riege 2003) and quotes were used as evidence when writing discussions to improve rigour (Dubé & Paré 2003).

5.3.3 Evaluation

Since I chose to interview experts experienced in implementing the ISO 27001 standard, the implementation process described by them followed the Plan-Do-Check-Act framework of this standard (illustrated in Figure 5.5). An InfoSec specialist implementing the ISO 27001 standard would begin with a risk assessment and design the InfoSec measures in the Plan stage, followed by the Do stage where the designed measures are implemented. Then, in the Check stage, they would perform the auditing and evaluation of the implementation's effectiveness and, in the Act stage, reflect on the evaluation and maintain the improvements (Gikas 2010; ISO 2017).

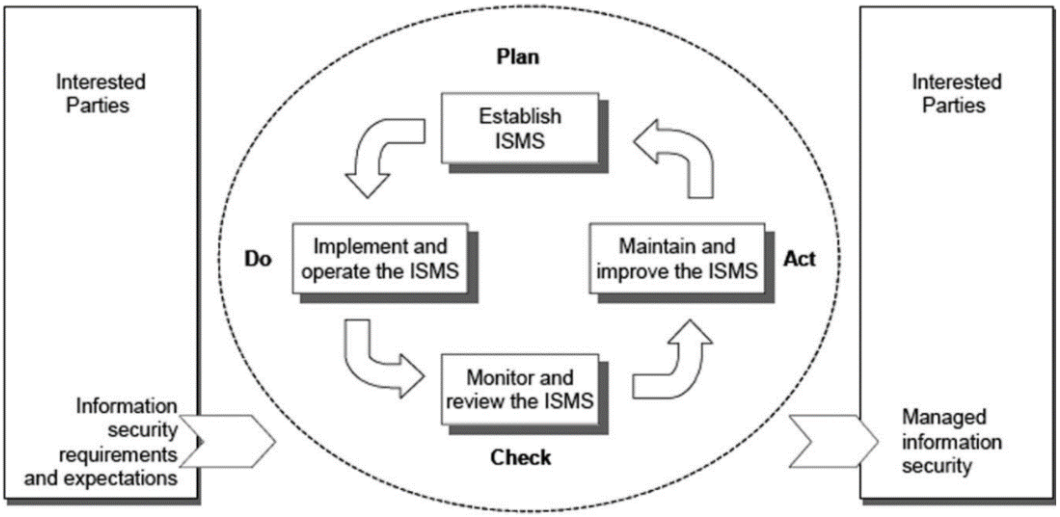


Figure 5.5. ISO 27001 Standard's Plan-Do-Check-Act Framework

Adopted from Gikas (2010, p. 136).

The critical factors for InfoSec implementation in Vietnamese context, which emerged from the within- and cross-case analysis on the interviews with the experts, were grouped into three themes. The first two themes focused on the critical factors that were recommended to be accounted for during the design and communication of the InfoSec implementation, and the third theme focused on the methods and tools to implement InfoSec in the workplace.

The grouping of the interviewed content's themes was based on the experts' common descriptions of a step-by-step InfoSec implementation process. For example, the critical factors 'practical, precise, and applicable InfoSec controls', 'collaboration between InfoSec team and department managers' and 'top management's financial and authoritative support' were consistently suggested by the experts when they discussed the Plan stage of the ISO 27001 implementation process. These factors focused on designing the implementation. Therefore, they were assigned to the first theme about the design of an InfoSec implementation.

Other critical factors, such as 'incentives of compliance', 'cost of compliance', 'InfoSec training' or 'sanctions' were mentioned when the interviewed experts discussed the Do, Check and Act stages of such implementation process. Moreover, when asked about the factors to be considered during these stages, the experts focused on the InfoSec-related contents that need to be communicated to end-users and how such communication should be facilitated. Consequently, this resulted in the second and third themes: 1) the factors that need to be considered during communication (e.g., Vietnamese and organisational cultures and the

communicated contents such as benefits and rewards) and 2) the methods or means to effectively communicate these contents.

The concepts, regarded as critical factors, were those that had many coded instances (i.e., the concept was explicitly mentioned many times by different experts). Table 5.5 summarises these critical factors and their themes, the number of experts who mentioned them and their number of coded utterance. Details of these critical factors supported by direct quotes are elaborated in the following sections.

Table 5.5. Critical Factors for InfoSec Implementation in Vietnamese Context

Theme	Critical factor	Description	Number of experts	Number of coded utterance
Designing InfoSec implementation	Practical, concise and applicable InfoSec measures	The three characteristics of InfoSec measures that affect the feasibility and effectiveness of their implementation.	6	47
	Top management's financial and authoritative support	The financial (e.g., allocation of budget for recruiting InfoSec personnel) and authoritative support (e.g., announcing the InfoSec policies and measures) from the top management that is essential for a successful InfoSec implementation.	6	37
	Collaboration between InfoSec team and department managers	A requirement for effectively implementing InfoSec improvements, especially in the design stage when the InfoSec team acquires feedback from the department managers to make the InfoSec measures practical and applicable.	5	20
Communicating InfoSec	Benefits of InfoSec compliance	The incentives (e.g., recognition, InfoSec knowledge) that can be communicated to employees to motivate their InfoSec compliance. The incentives can be explained as the benefits of InfoSec compliance for the organisations or for the individual employees.	6	33
	Costs of InfoSec compliance	The costs of complying with InfoSec policies and procedures (e.g., time and efforts) that needs to be considered when designing and implementing the InfoSec measures.	5	23

	Undesirable consequences of InfoSec violations or negligence	The undesirable consequences that can be communicated to employees to motivate their InfoSec compliance. The undesirable consequences can be explained as affecting the organisations and/or the individual employees.	6	32
	Sanctions	The punishments for InfoSec violations or careless behaviours. Some experts cautioned that mentioning sanctions too frequently may make employees feel threated and may result in negative results.	6	25
	Roles and responsibility	Every employee is responsible and accountable for organisational InfoSec by default. However, they may not realise their InfoSec roles and responsibility and the organisations need to explain the roles and responsibility to them.	6	42
	Vietnamese and organisational cultures	Traits of the Vietnamese culture (e.g., high collectivism and large power distance) and of the organisational culture (e.g., hierarchical nature) that need to be considered when implementing InfoSec improvements.	6	33
Methods and tools	InfoSec Training	The different approaches to conduct InfoSec training and the considerations to maximise the training effectiveness.	6	99
	Monitoring and evaluation	The audits and tests that are performed periodically to evaluate employees' InfoSec awareness and knowledge.	6	44
	Work interactions and social influence	The factors related to the work interactions (e.g., formal authority and peers' influence) and the use of opinion leaders that help persuade employees to comply with InfoSec policies.	6	97
	Agreements, technical restrictions and reminders	The measures such as posters, desktop screens, non-disclosure agreements and blocking websites or Facebook to promote InfoSec.	6	41

5.3.3.1 Critical factors for designing InfoSec implementation

This section describes the critical factors which contribute to an effective designing of an InfoSec implementation. Specifically, practitioners are advised to design InfoSec measures that are practical, concise and applicable for the work context, especially by closely collaborating with the department managers and by gaining financial and authoritative support from top management.

5.3.3.1.1 Practical, concise and applicable InfoSec measures

Most InfoSec experts emphasised three important characteristics to focus on when designing effective InfoSec measures which need to be practical, concise and applicable for each organisational context with its unique characteristics.

> *We had representatives of the departments to participate in the design process for the InfoSec policy and to give their feedback to make the policy more practical and applicable in the company's context. (EX2)*

> *If you enforce an InfoSec policy without taking into account the policy's relevancy to the company, then it will be very difficult to persuade people to follow it. (EX3)*

EX2 stressed that failures in InfoSec implementation often result from rigidly applying generic standards onto the organisation without thoughtful consideration. All interviewed experts recommended that InfoSec controls should be designed in a way that they are perceived by employees as useful and relevant to their department's operations and their own work. EX3 highlighted that all InfoSec controls must ultimately aim at meeting the expectations of top management, who are often the main sponsor investing in the implementation of InfoSec programs. Overall, the design and selection of the InfoSec controls to be implemented need to account for the needs and requirements of stakeholders at all levels.

5.3.3.1.2 Top management's financial and authoritative support

In the context of InfoSec implementation top management hold a vital role by providing their sponsorship, which affects the acquisition of the human and technical resources for an effective implementation. EX3 discussed a major challenge in top management often lacking knowledge of InfoSec controls and thus not willing to invest into InfoSec improvements. EX3 cited a case of an InfoSec implementation project in which top management of the company believed that the installation of a firewall alone would suffice for the company's InfoSec. EX3 found it

challenging to persuade top management to acquire more advanced InfoSec measures as they did not appreciate the benefits of InfoSec improvements. Similarly, EX6 emphasised the importance of informing top management about the benefits of InfoSec improvements to gain their support.

> *Top management's buy-in is extremely important for InfoSec implementation. (EX3)*

> *The second stage [designing the InfoSec implementation] is very important. The key activity in this stage is to present your implementation plan to the board of management, and you must convince them that the proposed InfoSec measures are crucial for the company and receive their support. (EX6)*

EX5 complained that top management in his firm saw InfoSec as consisting solely of technical measures. Therefore, his IT department did not receive a sufficient budget for a competitive salary package to attract InfoSec talents. Further, due to the budget constraint and top management's underestimation of InfoSec, it was not possible to conduct mandatory InfoSec training for all employees, but only on demand for a handful of departments. Moreover, the training was performed on EX5's own initiative and top management had reportedly never shown interest in maintaining the training periodically.

> *Large enterprises in Vietnam do have InfoSec departments that are dedicated to take care of InfoSec issues, but they mainly focus on the hardware, software, or network security…they have not yet realised the importance of the people and process components of InfoSec management. That's why they are not very supportive when it comes to training and enforcing procedures. (EX5)*

EX2 shared a similar experience in his early career, when top management ignored an InfoSec risk because they were not willing to allocate resources to mitigating that risk. This ignored risk subsequently led to an InfoSec breach.

> *Most top management of companies in Vietnam have not yet developed a mindset that sees InfoSec as important. It is understandable, since the companies in Vietnam still remain at the level of thinking about how to survive, rather than how to improve. (EX2)*

Apart from top management's allocation of resources to InfoSec implementation, their formal authority and critical roles were also discussed by the interviewees. Such authority could be used to enforce participation in InfoSec projects and to legitimise the implemented InfoSec controls. EX3 shared an experience of co-leading an implementation project with a company's representative who failed to have the other departments complete their assigned tasks on time.

After slow progress for three months, EX3 requested top management increase their presence in the project by attending the project meetings which immediately alleviated the issue.

5.3.3.1.3 Collaboration between InfoSec team and department managers

EX3 discussed that while top management contributes to InfoSec implementation by legitimising and enforcing InfoSec controls, InfoSec staff and department managers also play critical roles in designing InfoSec controls. EX6 discussed a previous InfoSec implementation project in which he required each department to jointly perform a risk assessment and to design the InfoSec controls with his InfoSec team so that the controls were aligned with department's operations and important assets.

> *The HR department has to manage personal information such as payrolls, so they need to be trained how to handle these confidential data. The sales department does not keep much personal data so they would not need to care much about privacy, but they often exchange information with third parties. Because of that they have to learn how to communicate information securely. (EX6)*

EX6 highlighted that only the participation of the department managers was required, not all employees, since gathering opinions from operational staff would make the project unnecessarily complex and hinder implementation. He remarked, 'It is impossible to design a process that satisfies everyone'. EX1 shared this view and explained that seeking department managers' insights would suffice for the InfoSec implementation as these managers have a thorough understanding about the business operations and a strategic vision that operational staff would not possess.

5.3.3.2 Critical factors for communicating InfoSec

After the InfoSec measures are designed and support from top management is acquired, the designed InfoSec measures and InfoSec-related contents must be effectively communicated to employees. EX2 highlighted the importance of communicating InfoSec to employees:

> *The main reason why employees are not motivated to comply with InfoSec policies is because you only force them to comply without explaining the reasons for compliance. When it lacks explanations, employees tend to create their own [negative] reasons, such as the companies want to restrict their freedom to use computers at work with the InfoSec policies. (EX2)*

This section presents the critical factors or the important InfoSec-related contents that practitioners are advised to communicate to employees during InfoSec implementation.

5.3.3.2.1 Benefits of InfoSec compliance

All InfoSec experts suggested informing employees about the benefits of InfoSec compliance to secure their acceptance of the implemented InfoSec controls. For example, EX1 listed the prevention of the productivity loss from an InfoSec breach as an advantage of InfoSec compliance. EX5 added gaining InfoSec knowledge as another benefit, by which employees can improve their knowledge and develop good InfoSec habits to protect their personal computers. EX3 mentioned a case where a company asked employees to participate in an InfoSec awareness test and those who achieved high scores had their names listed in the company's Hall of Fame. In this case, EX3 suggested that recognition can be another incentive for compliance.

EX6 argued that InfoSec compliance is not a voluntary decision, but an expected behaviour of organisation members and, therefore, does not require any incentives. While the InfoSec experts found it difficult to think about any personal benefits that employees could gain from InfoSec compliance, they suggested explaining to employees the incentives for InfoSec compliance which affect both themselves and their organisations. For example, EX1 suggested explaining that employees' InfoSec compliance would contribute to the protection of their departments' information assets and to their collective productivity. However, EX2 and EX3 contended that some employees would not care about the collective benefits of InfoSec:

> *The problem is, when someone said: 'If you don't comply with information security then you will risk the reputation of the company', then who cares? 'In the worst scenario, I'd just quit the company.' That's how most of them would think. (EX2)*

EX4 suggested a solution by establishing a mutual understanding about the benefits of InfoSec compliance for the organisations and for employees:

> *All benefits of compliance received by the company should be explained to the employees. When the company receives the benefits, then such benefits would be shared with the employees. For example, having good InfoSec makes our clients see us as more trustworthy, and they would give us more projects to work on. The company's revenue would then be generated and even increased, and so would the salaries or bonuses of the employees. (EX4)*

5.3.3.2.2 Costs of InfoSec compliance

All experts recognised that InfoSec compliance can be perceived as time-consuming and cumbersome for many employees, and that such costs of compliance pose a major obstacle to

achieve employees' InfoSec compliance. EX6 suggested that the costs of compliance can be minimised during the formulation stage where the design and selection of the InfoSec controls take place, while EX2 believed that the cost of compliance is inevitable regardless of how the InfoSec controls are designed:

> *There is no way that information security compliance is convenient. It is simply sacrificing the employees' convenience to secure the company's important assets. It's like keeping the valuables inside your house safe; it will be so much convenient if you don't have to lock the doors and windows when going outside, but you have to because you are afraid that your stuff will be stolen. (EX2)*

5.3.3.2.3 Undesirable consequences of InfoSec violations or negligence

Similar to the incentives for InfoSec compliance, the undesired consequences of InfoSec negligence or violation can be explained as affecting both the individual employees and their organisations to justify the importance of InfoSec controls. For example, EX1 suggested raising employees' InfoSec awareness by informing them of the consequences of not following an InfoSec policy.

> *There are several ways to motivate compliance by raising the employees' awareness that InfoSec incidents can impact their work directly. For example, if you work in the Accounting department then you need to lock your computer before leaving your desk. If you don't, anyone can easily delete your work on the balance sheets which usually take a lot of time and effort to prepare. (EX1)*

In addition to disciplinary actions as another personal undesired consequence of InfoSec negligence, all experts suggested placing emphasis on the InfoSec threats that target the organisation. EX3 and EX6 recommended that organisations should publish weekly news about InfoSec attacks and use them as case studies to raise employees' InfoSec awareness. EX6 highlighted that InfoSec threats at all levels of seriousness should be explained to employees.

5.3.3.2.4 Sanctions

The experts discussed the role of sanctions as a tool to enforce InfoSec compliance, which is used by practitioners and organisations that adopt the enforcement approach. Interestingly, EX1 and EX2 considered avoiding sanctions in the event of an InfoSec breach as an incentive for InfoSec compliance. Specifically, employees involved in InfoSec incidents could avoid sanctions if they present evidence of their compliance with prescribed InfoSec procedures.

While the interviewed experts agreed that communicating sanctions was necessary, they also cautioned:

> *Sanctions are communicated clearly in my company. If an employee violates the InfoSec policy then they will receive a warning for the first time. If they continuously receive warnings then they can have their salary and bonus reduced, or even get their contract terminated. (EX2)*

> *I always told my clients to avoid resorting to sanctions. What has happened has already happened; the primary objective of effective InfoSec controls is to prevent InfoSec incidents from happening. (EX3)*

Both EX1 and EX4 discussed that even mentioning sanctions without careful considerations could result in negative effects:

> *The more we emphasise sanctions, the more the employees will resist. Of course not everyone would protest against it, but I understand how the employees in my company feel...You would react when you are threatened, and that's natural. (EX4)*

5.3.3.2.5 Roles and responsibility

Although it is helpful to establish the incentives for InfoSec compliance and undesired consequences of InfoSec negligence, all experts shared the view that InfoSec compliance should be recognised by employees as part of their work roles and responsibility.

> *Being an employee of the company means that you have to follow its policies by default. (EX2)*

> *Everyone should know that they are responsible and accountable for the organisation's InfoSec. (EX3)*

> *We don't implement a rewarding system for InfoSec compliance in our company, because it is part of the policy and directives sent from our headquarters in Germany. Every employee must be aware of their responsibility in ensuring information security and comply with the policy. (EX6)*

The experts also agreed that the roles of InfoSec and responsibility for it involve not only personal compliance, but also the duty to educate other employees on InfoSec matters, especially if an employee holds a senior position. For example, EX1 had taken the 'train the trainers' approach and appointed department managers as champions whose roles then included acting as InfoSec role models and diffusing InfoSec knowledge among members of their departments. If these champions failed one of these tasks they would be held accountable for

it. In this context, EX6 highlighted the common issue that many Vietnamese employees are not aware of their personal InfoSec role and often expect that their colleagues' InfoSec compliance is sufficient for the organisation InfoSec.

5.3.3.2.6 Vietnamese and organisational cultures

All experts stated that the unique national and work cultures of Vietnam influence the use of tools and measures to implement InfoSec improvements. Therefore, they recommended practitioners to be aware of these cultural traits and make use of them to support the implementation of InfoSec improvements. For example, EX4 suggested using formal leaders at the appropriate levels of authority, depending on the hierarchical structure of the workplace, to inspire and motivate InfoSec compliance.

> *It depends on the culture of each organisation. There are companies where the top management are very close to the employees; so if these top executives can lead by example in their workplaces then it would be very effective. But if the power distance is too large then the immediate direct managers are more influential. (EX4)*

EX2 and EX6 posited that the industry that an organisation belongs also impacts how employees perceive the role of InfoSec, responsibility for it and the usefulness of InfoSec controls.

> *People who work in the banking sector would feel more comfortable with the security measures in place such as CCTVs and computer monitoring software. Because if a security incident occurred, they could show the recorded evidences that they were not responsible for the incident. (EX2)*

With regard to the Vietnamese culture, EX3, EX4 and EX6 complained about the low InfoSec awareness and knowledge of Vietnamese employees in general which affect the implementation of InfoSec improvements:

> *Vietnamese employees in general don't care about information security risks, since information security matters are rarely mentioned in educational programs and also in daily life. Vietnamese laws about information security are not clear and well-communicated to the citizens. That's why these people don't treat information security matters seriously. (EX6)*

EX3 argued that Vietnamese employees favour following the norms, reflecting the high collectivism in Vietnamese culture (Hofstede 2001), and suggested relying on this trait to diffuse InfoSec knowledge in the workplace. However, other experts believed that high

collectivism in a workplace with large power distance could jeopardise the consistent quality of InfoSec awareness and behaviours.

> *In some Vietnamese firms, information security policies are announced by the top management but enacted differently within each department, since the employees in these departments only follow their co-workers and direct managers but not those at the top level. (EX1)*

5.3.3.3 Methods and tools to communicate InfoSec

The interviewed experts categorised the implementation of InfoSec improvements into the persuasion and enforcement approaches. These two approaches should be flexibly applied to ensure employees' acceptance of the implemented InfoSec measures by communicating the InfoSec-related contents discussed in the previous section. Such communication aims at helping employees realise the priority of InfoSec which reflects top management's vision and explains to employees how InfoSec compliance would be personally meaningful to them. The tools and methods the experts recommended for communicating InfoSec are discussed below.

5.3.3.3.1 InfoSec training

Training was mentioned as the most common method to convince employees' InfoSec compliance by improving their InfoSec awareness and knowledge. Another purpose of training is to explain the enforcement mechanisms to employees to prevent any denial of responsibility. In interviews the experts presented 1) a large-scale approach training all employees in the same way, 2) a small group training approach targeting employees with similar roles and preferences and 3) the train the trainers approach which leverages champions' influence to diffuse InfoSec knowledge.

EX2 explained that the large-scale approach is generic and suitable for training newly hired staff, especially in large enterprises where there might be hundreds of new employees joining annually. The disadvantage of the large-scale approach is its generic nature which can be addressed by the small group approach. For example, EX2 argued that there exist groups of employees who have various levels of technical knowledge and needs and, thus, training should be tailored accordingly. Likewise, EX3 suggested that step-by-step instructions are especially useful for blue-collar workers whose computer proficiency might be low. Train the trainers was considered a form of the small group approach which leveraged the social influence of the key players to persuade others' InfoSec compliance.

The experts identified three critical factors of an effective training program, namely, the continuity and consistency of the program, employees' involvement in the training and the selection of the trainers. While the first characteristic is widely recommended by InfoSec standards such as ISO 27001, achieving the other characteristics requires more effort and a strategic vision from the InfoSec implementation team.

Most of the experts agreed on one method to encourage employees' involvement, which is making the training fun and interactive through facilitating open discussions and using small gifts or recognitions as incentives for employees' participation. EX3 highlighted that employees need to practise the handling of InfoSec issues in realistic scenarios relevant to their daily work. EX5 emphasised that employees must be encouraged to engage in discussions about InfoSec-related matters with the trainers during the training by actively questioning the trainers and exchanging information until employees truly understand the InfoSec issues. On the other hand, the experts disagreed about the selection of the InfoSec trainers. For example, EX3 advocated the use of external InfoSec trainers:

> *Internal trainers cannot train well for several reasons. For example, if you and I have been hanging out as colleagues, then suddenly you became my trainer, it's hard for me to see you as a teacher. However, when the company hires an expert from the outside with formal qualifications and experience, then it feels different. The external expert also has their unique way of teaching, and their experience also differs from what is happening in the company. That uniqueness triggers the learners' interest in learning with them. I also can't take my training lightly when learning with a stranger since I know he or she would not easily tolerate my mistakes. But to you who just went out for coffee with me, the effect won't be the same. (EX3)*

EX5 rejected the idea that companies should rely on external trainers, especially those based in Vietnam:

> *To me, as long as the internal trainers are knowledgeable and the employees' discipline is high, then they can conduct the training well. In fact, many InfoSec consulting firms in Vietnam are not even certified for delivering the programs that they offer to deliver. They can do all the fanciful presentations about their programs and fascinate the small and medium businesses, but large enterprises like us are demanding—we don't pay for their second-rate services and let them learn on the job. (EX5)*

5.3.3.3.2 Monitoring and evaluation

All experts recommended continuous monitoring and evaluation for implementation of InfoSec improvements. This includes the use of incident management systems to automatically monitor

employees' computers, periodical audits and online tests on the intranet to assess employees' InfoSec awareness and knowledge.

> *The basic measure to evaluate organisational InfoSec is the number of incidents, such as the number of detected virus, malware, DDOS, or when some internal employees tried to scan ports...we can monitor and record those incidents. (EX2)*

> *My company applies the 5S principles of the Japanese workplace organisation method. We also have a team that does periodical audits on things such as whether the desks and work documents are kept tidied. (EX5)*

Similar to conducting InfoSec training, EX4 suggested designing InfoSec tests as fun quizzes which reduce employees' perceived pressure of being formally evaluated and increase their voluntary participation. In contrast, EX1, EX2 and EX5 recommended making InfoSec tests compulsory and to have employees complete them with satisfactory scores. When being asked about the possibility of employees cheating in the InfoSec tests to achieve the satisfactory scores, EX1 did not see cheating as a serious issue. He explained that even when employees memorise answers from the last test or help their colleagues complete the test, such repeated cheating would help employees unconsciously learn about InfoSec. Both EX3 and EX6 suggested that audits should be carried out by internal staff since they understand the organisations' vulnerabilities and threats better than external auditors. EX6 argued that periodically conducting audits also displays the organisations' commitment to maintaining good InfoSec which could make employees realise that InfoSec is important and prioritised.

5.3.3.3.3 Work interactions and social influence

The experts put forward that InfoSec can be communicated via both formal training and employees' work interactions within the workplace. Most experts agreed that formal authority and organisational structures play a significant role in communicating InfoSec via daily work interactions. For example, although EX2 acknowledged that Vietnamese employees tend to follow the norms created by their colleagues' behaviours, he argued that organisations should not allow informal norms to prevail over formal communication channels such as through InfoSec staff or authoritative managers. On this basis, all experts except EX5 saw informal opinion leaders and norms as contributing little to communicating InfoSec:

> *Having informal opinion leaders is not practical. If there are so many formal and informal information security leaders in a workplace, then who should listen to whom? (EX2)*

We don't use opinion leaders to persuade information security compliance. Since the nature of information security is being predominantly perceived as highly technical, you need to leave the persuasion to only a few technical persons to gain people's trust. There would not be many people in an organisation who fit that role. (EX3)

Honestly speaking, I don't see colleagues' behaviours and attitudes as important, because information security compliance ultimately depends on one's own awareness. If they are well-trained and have good awareness then they can perform the information security behaviours well, even when they work in an environment where the majority fail to do so. (EX6)

I think having opinion leaders is beneficial. If there are some key employees who are seen by others as role models, and they can showcase that they perform InfoSec practices well then that positive image will spread within the workplace. (EX5)

The experts' lack of consensus on the use of informal opinion leaders suggested that such a tactic may be feasible in practice, but only when certain requirements are met. To this end, I probed into these requirements by enquiring about the desirable characteristics of an effective InfoSec opinion leader.

EX2 and EX3 both explained that InfoSec leaders must possess a balanced set of knowledge of both InfoSec and business matters and good leadership and communication skills. All experts emphasised the effective practice of leading by example to motivate other employees' InfoSec compliance. As department managers are in the position where they constantly develop and display leadership, they were considered as potential candidates for the diffusion of InfoSec knowledge. EX2 further suggested making use of department managers' close relationship with other department members to better convince them about InfoSec compliance and to deliver clearer InfoSec instructions which might complement the InfoSec training.

5.3.3.3.4 Agreements, technical restrictions and reminders

The use of formal agreements and reminders was mentioned by the experts as the means to reinforce employees' InfoSec compliance. For example, the experts reported the use of the non-disclosure agreements to inform employees about the role of InfoSec and their responsibilities. Although contracts and agreements can clearly communicate InfoSec requirements to employees, EX2 stated that employees can be overloaded by and ignore the information in those agreements.

Employees need to receive frequent InfoSec-related information via emails or via their line managers, and they have to sign their agreements to InfoSec policies and

prescribed procedures. At the same time, we also have measures to promote InfoSec-related matters such as posters and desktop screens. (EX2)

EX1 and EX5 suggested using technical restrictions to enforce InfoSec compliance such as blocking online social media or websites, managing access rights to files and folders or setting automatic reminders for changing passwords.

Together with persuading the employees to comply with information security policies, there are technical measures such as assigning access rights and blocking websites or Facebook to further mitigate information security risks. (EX5)

Posters, desktop screens, banners and announcements were also considered by the experts as effective means for reminding and promoting the importance of InfoSec compliance. While EX2 thought that the deployment of these tools was easy, he also contended that measuring their effectiveness in communicating InfoSec would be difficult. As such, he recommended practitioners to not overly rely on these tools.

5.4 Reflection

In this diagnosis stage I performed two research actions: 1) diagnosed the InfoSec issues at TTT and 2) investigated the critical factors and best practices for implementing InfoSec programs in the Vietnamese context. The risk assessment revealed that TTT currently encountered many issues related to employees' inadequate InfoSec knowledge. Moreover, the identified factors and best practices were found useful for designing the InfoSec change program at TTT. The following sections present my reflection on the findings resulting from the research actions and determine the next course of action.

5.4.1 Reflection on the Issues Related to InfoSec Climate at TTT

After reviewing the InfoSec issues at TTT, the project team and top management reached a consensus that the envisioned InfoSec change program should focus on improving employees' InfoSec knowledge and awareness. Reflecting on the focal theoretical concept of InfoSec climate (Ashforth 1985; Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Schneider & Reichers 1983), we concluded that no InfoSec climate currently existed at TTT because InfoSec had never been treated as a priority in the workplace. Additionally, the identified issues from the risk assessment such as the lack of InfoSec training and employees' insecure InfoSec behaviours indicated that InfoSec-related activities had not taken place at TTT. In line with the

theoretical explanations about the formation of InfoSec climate the project team determined that the InfoSec change program needed to increase the InfoSec-related socialisation between employees to form a positive InfoSec climate. Moreover, we concluded that TTT could also leverage this socialisation to diffuse InfoSec awareness and knowledge in the workplace. To this end, the interviews with the InfoSec experts offered the critical factors and methods to effectively communicate InfoSec to employees.

5.4.2 Reflection on the Critical Factors and Methods for Implementing an InfoSec Change Program at TTT

The critical factors and methods for InfoSec implementation in the Vietnamese context, identified through the interviews with the InfoSec experts, mirrored those recommended by prior research. For example, prior studies emphasised the impact of clarity and applicability of InfoSec controls on InfoSec compliance (see e.g., Boss et al. 2009; Höne & Eloff 2002; Karyda, Kiountouzis & Kokolakis 2005; Ruighaver et al. 2007). Spears (2006) and Spears and Barki (2010) also highlight the importance of user participation during InfoSec implementation, especially in the risk assessment stage. The project team successfully gained buy-in from the department managers by involving them in the risk assessment. The top management also realised the analytical capabilities of SNA methods through the analysis of the risk network and supported the use of these methods to analyse and improve the InfoSec-related socialisation between employees. As such, I found the current situation favourable for the subsequent implementation of the InfoSec change program.

The project team considered the experts' suggestion to make use of the daily work interactions and social influence, which leveraged the high collectivism of Vietnamese culture, to encourage employees' InfoSec compliance. Top management also agreed with following this persuasive approach as the work culture at TTT had been relying on persuasion to facilitate employees' acceptance of organisational changes rather than enforcing changes with strict rules. This reinforced the project team's intention to enhance the InfoSec environment in TTT by improving the InfoSec-related socialisation which would contribute to the formation of a favourable InfoSec climate. To this end, the project team took note of the experts' recommended criteria to select InfoSec leaders suitable for the persuasive diffusion of InfoSec knowledge. According to the experts, InfoSec leaders should have a balanced mindset of business and InfoSec matters, leadership and communication skills and the ability to lead by

example. This subsequently suggested that the project team would need to conduct InfoSec training for the selected leaders.

Recognitions and tangible rewards were recommended by the experts and by prior research as incentives that motivate employees' InfoSec compliance (Boss et al. 2009; Pahnila, Siponen & Mahmood 2007; Ruighaver, Maynard & Chang 2007). Moreover, the experts suggested explaining the benefits of InfoSec compliance and undesired consequences of InfoSec negligence, which impact both employees and their organisations, to help employees fully understand the importance of InfoSec. The use of sanctions as a deterrent of misbehaviours originated from GDT (Straub 1990) and as employees' motivation to comply with InfoSec policies was supported by empirical studies (see e.g., Guo & Yuan 2012; Herath & Rao 2009a; Siponen, Pahnila & Mahmood 2007). Likewise, sanctions were identified by the experts as a critical factor for implementing InfoSec programs. Contrary to my initial belief that an enforcement approach would be most suitable for ensuring InfoSec compliance in the Vietnamese context where many employees are not familiar with InfoSec, the experts put emphasis on persuading employees to comply with InfoSec policies. Although the experts recognised sanctions as necessary, they advised to not overly emphasise sanctions when communicating InfoSec to employees since this may result in negative effects by making employees feel threatened. The project team decided to take these insights into account when deciding the communicated InfoSec-related contents in this project.

5.4.3 Reflection on the InfoSec Implementation Approach at TTT

The project team and top management identified from the interviews three approaches to communicate InfoSec to employees—the large-scale, small group and train the trainers approaches. The large-scale approach is generic in nature and particularly useful for training a large number of employees in a timely manner. This approach was deemed least favourable by the project team, since TTT neither had a tried-and-tested InfoSec training program nor the experience to ensure the success of a one size fits all solution. Moreover, each of the departments at TTT had their own operations and subculture, meaning that a generic implementation approach would ineffective.

The small group approach, which divides the organisation's population into smaller groups of employees (e.g., based on computer expertise or work roles) and tailors the training programs according to the participants' common characteristics, was considered to have more potential

than the large-scale approach. The train the trainers approach is a special form of the small group approach which makes use of opinion leaders to diffuse InfoSec knowledge to their local communities. Train the trainers approach was considered as most favourable since it satisfied the need to flexibly customise InfoSec training programs to suit different contexts. Moreover, the approach aligned with TTT's organisational culture which relied on interpersonal influence and persuasion. This approach offered more benefits than the small group approach since it not only improves InfoSec awareness of employees in general, but also provided TTT with a group of opinion leaders who would continue to maintain the InfoSec climate in the long run. The adoption of this approach was also most feasible, given the limited resources and time frame of a PhD candidature. Finally, I considered that performing SNA to identify the informal InfoSec leaders would create more opportunities to produce new scholarly knowledge. Therefore, the project team and top management agreed to follow the train the trainers approach to implement the InfoSec change program at TTT. The research actions of the next action planning stage were also decided to focus on identifying these influential trainers or InfoSec leaders.

5.5 Chapter Summary

This chapter described the commencement of the CAR project in collaboration with TTT, in which two research actions of the project's diagnosis stage were performed. First, risk assessment activities, inspired by the InfoSec standard ISO 27001, were conducted with the department managers in TTT to diagnose the current InfoSec issues in their work environment. The risk assessment's results clearly indicated that the major InfoSec issues were related to employees' inadequate InfoSec awareness and knowledge. Moreover, the project team established that an InfoSec climate did not currently exist at TTT's workplace as the priority of InfoSec and InfoSec-related activities had never been promoted. As a result, these findings suggested that the InfoSec change program should increase employees' InfoSec-related socialisation to form a favourable InfoSec climate while leveraging this socialisation to diffuse InfoSec knowledge to employees. I demonstrated the analytical capabilities of the SNA methods to top management by visualising and analysing the InfoSec risk network. Conducting the risk assessment with the department managers also helped me acquire their buy-in for the InfoSec change program.

The second research action aimed at understanding the critical factors of InfoSec implementation in the Vietnamese context. A case study and interviews with six external

InfoSec experts (in charge of implementing the ISO 27001 standard for their companies in Vietnam) were conducted. The motivation of this second research action was to increase the project team's knowledge of implementing InfoSec improvements, contributing to the effective design of the project's subsequent interventions. Thirteen critical factors and methods were identified from the interviews with the InfoSec experts, consistent with the findings of prior research. The experts further recommended three approaches to communicate InfoSec to employees, of which the project team chose the train the trainers approach which leverages opinion leaders to diffuse tailored InfoSec knowledge to small groups of employees. The summary of this chapter's diagnosis stage is shown in Figure 5.6.

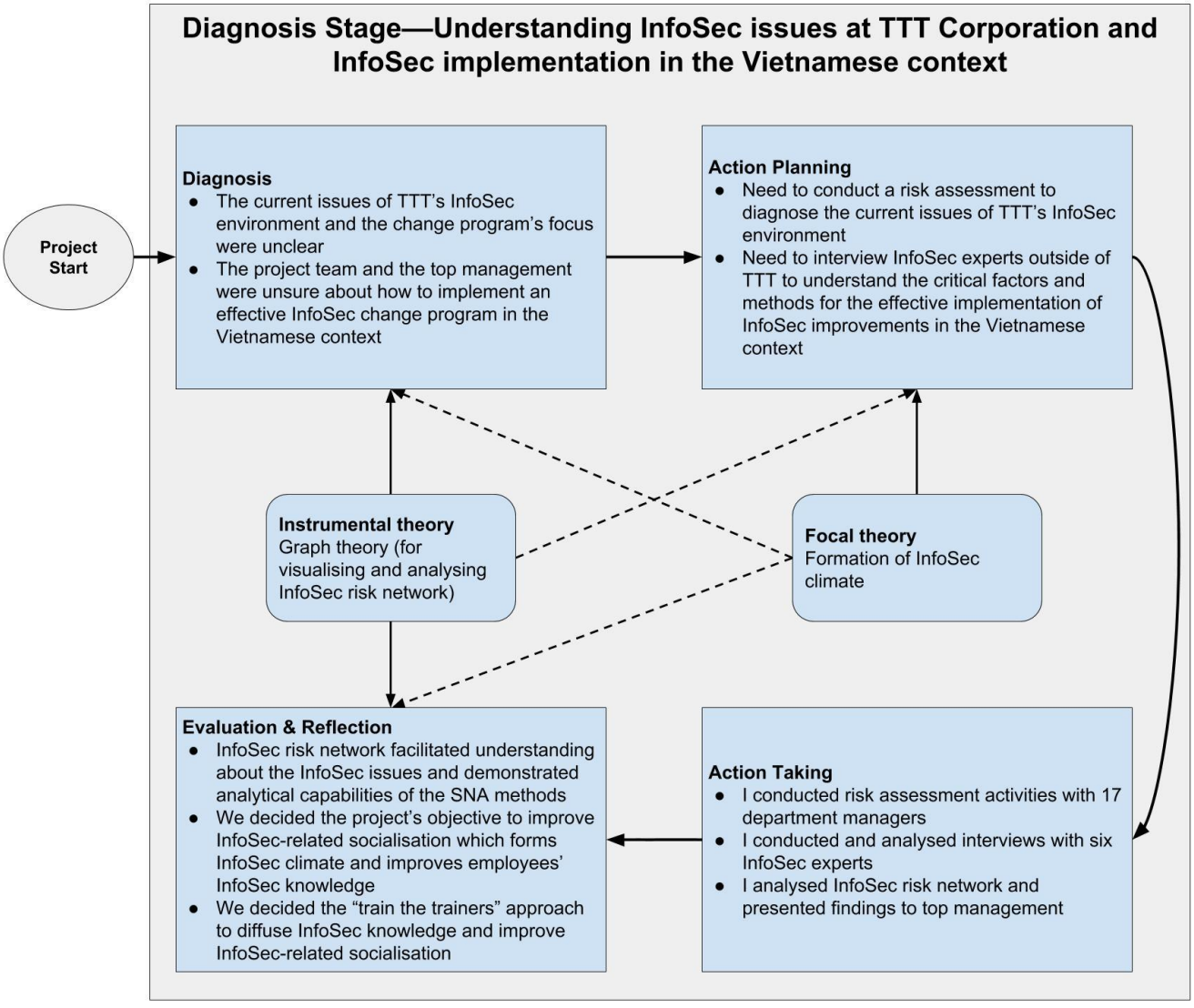


Figure 5.6. Summary of the Diagnosis Stage

Chapter 6: Action Planning Stage—Investigating InfoSec Environment before the Change Program and Identifying Champions for InfoSec Diffusion

This chapter discusses the action planning stage of the CAR project. The stage began with a diagnosis which took into considerations the project team's previous intention to follow the train the trainers approach to diffuse InfoSec knowledge in TTT. Next, I reviewed the relevant theories to support the identification of the influential trainers or InfoSec champions and research actions were taken in the action taking stage.

ERGM was performed to determine the characteristics that made an employee capable of influencing another employees' InfoSec behaviours. The results of this analysis were discussed at the end of this stage. Based on the identified characteristics of InfoSec-influential employees 50 champions were selected. The chapter concludes by presenting the reflections on the iteration's outcomes. Figure 6.1 summarises the structure of this chapter.

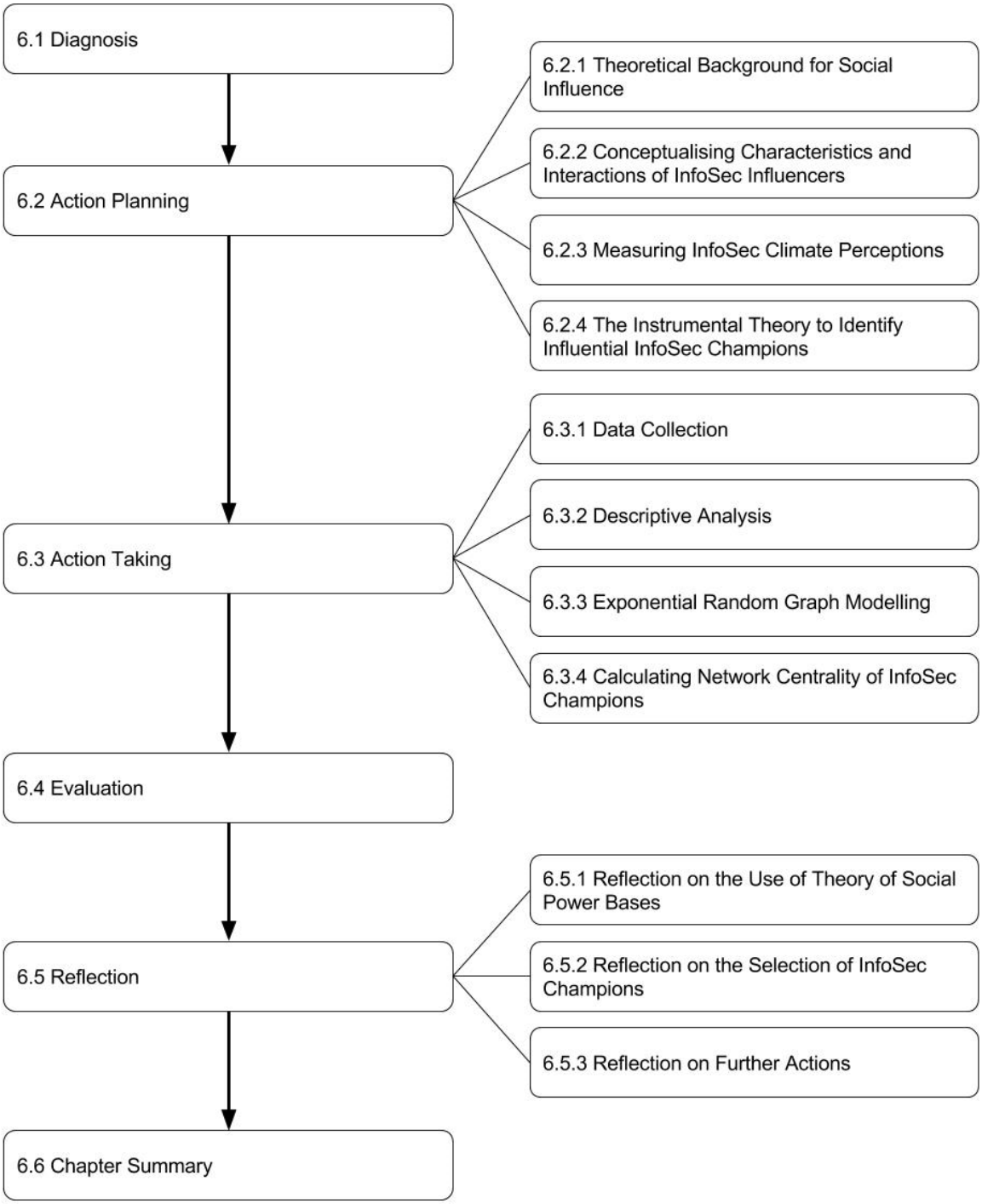


Figure 6.1. Structure of Chapter 6

6.1 Diagnosis

The risk assessment described in Chapter 5 identified the major InfoSec issues at TTT—employees' inadequate InfoSec knowledge and InfoSec awareness. Findings from the interviews with InfoSec experts, who oversaw InfoSec implementation for their companies, revealed the critical factors and methods to improve InfoSec environments in the Vietnamese

context. These findings presented the best practices that the project team considered for designing the InfoSec change program at TTT.

The project team together with top management decided at the end of the diagnosis stage that the InfoSec change program should focus on improving the InfoSec-related socialisation between employees to improve the InfoSec climate at TTT. This was in line with the theoretical explanations about the formation of InfoSec climate (Ashforth 1985; Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Schneider & Reichers 1983) and would allow the project team to leverage the socialisation to diffuse InfoSec knowledge and awareness. The project team and top management had also decided to follow the train the trainers approach that leverages influential opinion leaders in the workplace to diffuse InfoSec knowledge. The decision to follow this approach was aligned with the organisational culture of TTT, which relied on interpersonal influence and persuasion, and with the limited time frame of the project.

Even though the project team and top management had agreed to follow the train the trainers approach to diffuse InfoSec knowledge, we did not know how to identify the opinion leaders who would perform the diffusion. We discussed that the department managers could take the leader role and rely on their formal authority to perform the diffusion, but such a diffusion task would add an extra burden to their heavy workload. The department managers were busy with their managerial tasks which left them little time to provide other employees with immediate InfoSec support. Moreover, it would be more beneficial in the long term to have operational staff acting as InfoSec champions and maintaining the diffusion of InfoSec in their departments. We also anticipated that having department managers and operational staff share the responsibility to diffuse InfoSec knowledge would also increase the speed of diffusion and improve the collaboration between the department managers and the operational staff. As such, we decided to select both department managers and operational staff at TTT to be the opinion leaders for the diffusion.

The project team and top management decided to adopt SNA methods to identify the InfoSec champions for the diffusion of InfoSec knowledge. For TTT, it was imperative to have an evidence-based design of the intervention and a set of well-defined criteria for evaluating the intervention's effectiveness. To this end, the adoption of SNA methods was justified as these methods produce quantitative measures that characterise the potential InfoSec leaders' social prominence and the structural features of the InfoSec-related socialisation. Based on these measures, potential InfoSec leaders for the train the trainers approach would be selected. The

top management had acknowledged the analytical capabilities of the SNA methods for the identification of non-human entities such as InfoSec threats and vulnerabilities and they were willing to support the adoption of these methods to analyse the InfoSec-related socialisation between employees. The adoption of SNA methods, which enabled the identification of InfoSec champions regardless of their formal and informal status, also made the InfoSec implementation feasible in the context of the project's limited resources and time frame. Further, performing SNA contributed to my scholarly objective of exploring the applications of SNA methods in the behavioural InfoSec field.

6.2 Action Planning

Based on the knowledge about the use of SNA methods to identify the critical threats and vulnerabilities in the diagnosis stage, the project team and top management planned to select InfoSec champions who held prominent positions in TTT's networks of work and InfoSec-related interactions. This plan required careful considerations to determine the relevant networks for analysis.

In line with the objective to identify the champions for the diffusion of InfoSec knowledge and CAR's principles (Davison, Martinsons & Ou 2012) I selected the focal and instrumental theories that supported the mentioned plan. The focal theories should focus on the characteristics and behaviours that enable an employee to be recognised by other employees as InfoSec influencers, while the instrumental theories should inform the methods to identify these influential employees in a workplace. By reviewing these theories, I also aimed to determine the relevant networks of the work interactions which facilitate employees' recognition of each other as InfoSec influencers.

The next sections review the literature to identify the relevant networks and employees' characteristics that facilitate InfoSec influence between employees. After the relevant networks and employees' characteristics were identified, I designed a questionnaire to capture these networks and characteristics. Consistent with my scholarly objective, I also designed questions to capture employees' perceptions of an InfoSec climate.

6.2.1 Theoretical Background for Social Influence

Social influence and its role in the behavioural InfoSec field have been confirmed in a number of studies (Lebek et al. 2014; Padayachee 2012; Sommestad et al. 2014). For example, many

studies have identified subjective norms to motivate employees' InfoSec compliance (Bulgurcu, Cavusoglu & Benbasat 2010a; Ifinedo 2014; Leonard, Cronan & Kreie 2004; Safa et al. 2015). This concept belongs to TPB (Ajzen 2011b), which posits that a person's decision to perform InfoSec behaviours is affected by the social influence exerted by the people deemed important to them. Other effects related to social influence such as social bonds and group sanctions were also found to affect InfoSec behaviours (Guo & Yuan 2012; Ifinedo 2014). However, these studies only confirmed the effects of social influence on InfoSec behaviours or perceptions; they did not determine the characteristics that make employees capable of influencing other employees' InfoSec perceptions and behaviours. Thus, practitioners have limited knowledge about the methods for creating the social influence that shapes desirable InfoSec perceptions and behaviours in organisations.

Kelman (1961) discussed that social influence operates through three processes—internalisation, compliance and identification. Internalisation focuses on the behaviour's characteristics rather than on the human influencer, and thus the examination of this process is less relevant to this CAR project's objective to find the personal characteristics of influential individuals. Compliance occurs when a person accepts the influence in the belief that doing so would result in a favourable reaction from the influencer, while identification refers to the individual's acceptance of the influence to maintain their relationship with the social groups and a sense of identity (Cialdini & Goldstein 2004; Kelman 1961). The motivation of compliance is often the need to avoid a punishment or receive a reward (Burnkrant & Cousineau 1975), which has been studied in the InfoSec context (Guo & Yuan 2012; Siponen, Mahmood & Pahnila 2014). Likewise, prior InfoSec studies have investigated the relationship between a person's identification of an InfoSec behaviour and their intention to perform InfoSec behaviours in the form of organisational commitment (Lebek et al. 2014).

The theory of social power bases (French & Raven 1959; Raven 2008) elaborates on the types of power bases that make a person appear influential to others—expert, referent, reward, coercive and legitimate power. Reward and coercive powers are consistent with Kelman's (1961) framework of social influence, which refers to a person's ability to give rewards and/or punishments for a behaviour. This ability influences other people to comply with the prescribed behaviour. Referent and legitimate powers are represented by a person's status, deemed by the influenced targets as deserving of their acceptance of the influence. Such status of an influential person may come from their impression as an admirable role model, a formal authority or a

required obligation by default as dictated by social norms. Finally, expert power may be automatically granted by acquired qualifications of an expert or by interactions in the workplace that help the influenced targets recognise the influencer's superior expertise.

The theory of social power bases (Raven 2008) outlines the specific traits and abilities that enable a person to exert social influence over other people. The theory also outlines behavioural cues of interpersonal influence, such as employees' provision of information, that are observable. Thus, influential champions could be identified by the project team based on these behavioural cues and monitor their observable changes to evaluate the champions' diffusion. The theory of social power bases has not appeared in recent studies in the behavioural InfoSec field (Lebek et al. 2014; Padayachee 2012; Sommestad et al. 2014; Warkentin & Mutchler 2014), suggesting an opportunity for generating new scholarly knowledge by examining the theory. On this basis, the project team agreed to adopt the theory of social power bases as the focal theory of this stage.

6.2.2 Conceptualising Characteristics and Interactions of InfoSec Influencers

The theory of social power bases (Raven 2008) explains how a person can exert influence over another person by possessing certain traits and abilities. The theory posits that a person's influential status is created by the abilities to inform others with their knowledge (i.e., informational and expert powers), acquire others' compliance by using rewards or punishment or simply appear as a role model (i.e., referent power) (Raven 2008). From a network perspective, these abilities can be analysed in the form of the socialisation (ties) between employees (nodes) in a network.

SNA studies have examined social influence that occurs via direct communication with others (Burt 1987; Leenders 2002) which can be facilitated via instrumental and expressive networks (Ibarra & Andrews 1993; Saint-Charles & Mongeau 2009; Umphress et al. 2003). Instrumental networks refer to the provisions of job-related resources such as work advice, while expressive networks refer to the provisions of non-work resources such as friendship and social support (Johnson-Cramer, Parise & Cross 2007; Fombrun 1982; Ibarra 1993; Parise 2007; Saint-Charles & Mongeau 2009; Tichy, Tushman & Fombrun 1979).

In this research, instrumental networks consisted of the provision of work advice that helps an employee overcome a work problem or improve their work efficiency (i.e., professional advice), and of the provision of organisational updates about the changes in work procedures

and policies (i.e., job-related information). The project team took into consideration the sharing of organisational updates because InfoSec requirements are often introduced to employees as an embedded component in their regular work processes, especially to instruct how organisational resources should be used (Ifinedo 2012). Employees actively seek experts in their instrumental networks to reduce uncertainty and make sense of the work environment (Saint-Charles & Mongeau 2009). Through providing work advice and organisation updates, the providers demonstrate their informational or expert power, and thus exert social influence over the receivers of these advice and updates (Raven 2008).

Expressive networks play significant roles in facilitating the social functions of organisations by complementing the job-related instrumental networks (Johnson-Cramer, Parise & Cross 2007; Ibarra & Andrews 1993). Expressive networks allow individuals to choose role models and referents that subsequently influence perceptions and behaviours due to their social power bases (Raven 2008). Individuals tend to have their perspectives about job and organisation influenced by others as they engage in expressive networks of interpersonal trust (Ibarra & Andrews 1993; Umphress et al. 2003; Zhou, Siu & Wang 2010). In this context, McKnight (2002) proposed four main types of trusting beliefs—1) competence, 2) benevolence, 3) integrity and 4) other traits such as predictability, openness, carefulness and attraction—where a trustworthy person demonstrates that they are competently reliable and capable of providing social support.

The project team also investigated the provisions of InfoSec advice and InfoSec troubleshooting support as networks (Dourish et al. 2004; Safa, von Solms & Futcher 2016; Warkentin, Johnston & Shropshire 2011). We decided to examine employees' provisions of InfoSec advice and troubleshooting support as these InfoSec-related resources assist employees in successfully performing the InfoSec practices required by the company. The providers of InfoSec advice and troubleshooting support possess both an informational power base (Raven 2008) and the opportunities to exert InfoSec influence over other employees via direct communication (Leenders 2002). Moreover, these networks represented employees' InfoSec-related socialisation that contributes to the formation of InfoSec climate (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013).

In addition to the influence arising from the active provisions of organisational resources, social influence can occur through the sharing of physical locations and affiliations that facilitate such provisions (Borgatti, Everett & Johnson 2013; Ibarra & Andrews 1993; Lusher, Koskinen &

Robins 2012). Borgatti and Cross (2003) found that sameness of gender and physical proximity result in information seeking among employees. A homophily effect, which results in people choosing to associate and be influenced by each other, is explained by similarities in demographics such as age and occupation (McPherson, Smith-Lovin & Cook 2001). Further, a legitimate power base is often gained from the formal authority of seniority at work (Ibarra & Andrews 1993; Raven 2008). Similarly, employees with longer tenure are often considered to possess more work knowledge which allows them to influence others, especially newcomers, more easily (Borgatti & Cross 2003).

Based on the discussed theoretical background about employees' characteristics and socialisation that lead to social influence, I developed a network questionnaire for collecting data. To improve validity of the questions, I consulted the opinions of the Vice Director of the BSP department and of top management to ensure the questions would capture the intended networks. The questions also provided examples of what was considered as work-related advice, personal advice or InfoSec-related resources so that the respondents could understand and answer the questions accurately. The details about the questions to collect network data are summarised in Table 6.1.

Employees' background characteristics (i.e., age, gender, department membership, seniority and tenure) were downloaded from TTT's HR database. The network of InfoSec influence was included as the predicted outcome of this stage's analysis to identify influential InfoSec champions for the diffusion of InfoSec knowledge by determining the characteristics that make a person influential in the InfoSec domain.

Table 6.1. Questions about Networks

Higher-order network	Transposed network	Network question
Instrumental network (provisions of job-related resources)	Give work advice network	Who do you usually ask for advice (e.g., look for or improve solutions, get referrals or confirmation) about work?
	Give organisational updates network	From whom do you usually get the latest updates or changes (e.g., new policies, processes and systems) in TTT?
InfoSec support network	Give InfoSec advice network	Who would explain the importance of InfoSec to you and/or teach you how to perform InfoSec behaviours and/or use InfoSec technologies?

(provisions of InfoSec advice and InfoSec troubleshooting support)	Give InfoSec troubleshooting support network	When you encountered an InfoSec problem (e.g., lost or damaged data, computer virus infection, etc.), whom would you seek help from?
Expressive network (provisions of trust and personal support)	Give personal advice network	When you want to discuss or ask for advice about personal life issues, whom would you talk to?
	Trust in expertise network	Who do you think would be most able (because of education, experience, qualities) to take over your work if you were too busy or absent?
InfoSec influence network	InfoSec influence network	In general, your decision to perform InfoSec behaviours, use technologies and/or exercise InfoSec care, etc. in daily work would be influenced by whom?

6.2.3 Measuring InfoSec Climate Perceptions

This section elaborates on the concept of InfoSec climate and its measurement in this project. Two sets of questions were designed based on prior studies to capture respondents' perceptions of InfoSec climate and these questions were added to the same questionnaire containing the questions listed in Table 6.1. The analysis of InfoSec climate is not described in this action planning stage; it is described in the final evaluation and reflection stage, where longitudinal data about employees' networks and InfoSec climate was captured after the champions' diffusion of InfoSec knowledge.

The concept of InfoSec climate refers to employees' perceptions of the InfoSec behaviours performed by their colleagues and direct supervisors which indicate the organisation's priority of InfoSec (Chan, Woon & Kankanhalli 2005; Lowry & Moody 2013). Chan, Woon and Kankanhalli (2005) were the first researchers who defined InfoSec climate by adapting the relevant and established concept of safety climate which focuses on the observable practices that inform how much organisations prioritise to ensure workplace safety (Zohar 2014). Zohar defined safety climate as follows:

> *[…] safety climate relates to shared perceptions with regard to the priority of safety policies, procedures, and practices and the extent to which safety compliant or enhancing behavior is supported and rewarded at the workplace. (Zohar 2014, p. 318)*

Building on this and Campbell and Beaty's (1971) work on organisational climate, Chan, Woon and Kankanhalli (2005), defined InfoSec climate as:

> *Perceived information security climate is defined as the employee's perception of the current organizational state in terms of information security as evidenced through dealings with internal and external stakeholders (Campbell & Beaty 1971). Perceptions of the climate are derived from observance of organizational management, superior, and peer attitudes. (Chan, Woon & Kankanhalli 2005, p. 25)*

Both InfoSec and safety climate are specific forms of the climates that coexist within an organisation, each of which focuses on a particular organisational facet (Schneider & Reichers 1983). For example, prior studies have investigated specific organisational climates such as involvement climate, service climate, innovation climate, justice climate and others (Kuenzi & Schminke 2009). Despite having different foci, these climates share commonalities in their nature as perceptual constructs that describe collective phenomena (Kuenzi & Schminke 2009).

While behavioural InfoSec studies have predominantly investigated employees' individualistic cognition and behaviours, InfoSec perceptions and behaviours also have collective characteristics (Dourish & Anderson 2006). The concept of InfoSec climate highlights such collectivistic nature as it explains that employees' perceived priority of InfoSec in the workplace is shaped by the InfoSec practices that they observe from their colleagues and supervisors (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013). Since each employee's interpretation of the surrounding InfoSec environment is subjective, InfoSec climate is perceptually constructed rather than representing objective InfoSec features of the workplace. Moreover, InfoSec climate emphasises the perceptions of the observable InfoSec environment rather than the underlying assumptions, beliefs or values of an InfoSec culture deeply ingrained in the organisation (Furnell & Thomson 2009; van Niekerk & von Solms 2010; da Veiga & Eloff 2010).

Following the existing operationalisation of InfoSec climate (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013) and its relevant safety climate (Brondino, Silva & Pasini 2012; Brondino, Pasini & Costa 2013; Kines et al. 2011; Lingard, Cooke & Blismas 2009; Zohar & Luria 2005), the project team developed two sets of questions to capture employees' climate perceptions of their colleagues and direct supervisors' InfoSec behaviours (summarised in Table 6.2). The rating scales of all questions had seven points, ranging from 'Never' to 'Always', to measure the frequency of the observed InfoSec

behaviours and from ‘Never’ to ‘A great deal’ to measure the intensity of the observed InfoSec behaviours.

Table 6.2. Questions about InfoSec Climate Perceptions

Construct	Question (measurement item)	Anchoring points	Adapted sources
Perception of direct supervisors’ InfoSec behaviours (SUP)	How frequently do your direct supervisor(s) mention about InfoSec matters to you and your colleagues? (SUP1)	Never; Very rarely; Rarely; Sometimes; Occasionally; Very frequently; Always	Chan, Woon and Kankanhalli (2005); Goo, Yim and Kim (2014); Jaafar and Ajis (2013)
	How much do your direct supervisor(s) ask that you and your colleagues in the work unit perform InfoSec behaviours? (SUP2)	Never; Very Little; Little; Somewhat; Much; Very much; A great deal	Kines et al. (2011); Zohar and Luria (2005)
	How frequently do your direct supervisor(s) discuss InfoSec threats with you and your colleagues? (SUP3)	Never; Very rarely; Rarely; Sometimes; Occasionally; Very frequently; Always	Chan, Woon and Kankanhalli (2005); Goo, Yim and Kim (2014); Jaafar and Ajis (2013)
	How serious, strict, or careful are your direct supervisor(s) when it comes to protecting InfoSec? (SUP4)	Never; Very Little; Little; Somewhat; Much; Very much; A great deal	Zohar and Luria (2005)
	How frequently do your direct supervisor(s) allow you and your colleagues to overlook InfoSec when rushing deadlines? (SUP5) (reversed)	Never; Very rarely; Rarely; Sometimes; Occasionally; Very frequently; Always	Brondino, Silva and Pasini (2012); Brondino, Pasini and Costa (2013); Kines et al. (2011); Zohar and Luria (2005)
Perception of colleagues’ InfoSec behaviours (COL)	How much do your colleagues perform InfoSec behaviours in their daily work? (COL1)	Never; Very Little; Little; Somewhat; Much; Very much; A great deal	Kines et al. (2011)
	How much do your colleagues care about InfoSec? (COL2)	Never; Very Little; Little; Somewhat; Much; Very much; A great deal	Jaafar and Ajis (2013)
	How much training and updates about InfoSec do your colleagues receive? (COL3)	Never; Very Little; Little; Somewhat; Much; Very much; A great deal	Goo, Yim and Kim (2014)

	How much do your colleagues prioritise InfoSec when they are rushing deadlines? (COL4)	Never; Very Little; Little; Somewhat; Much; Very much; A great deal	Chan, Woon and Kankanhalli (2005); Jaafar and Ajis (2013); Lingard, Cooke and Blismas (2009)
	How much do your colleagues pay attention to and perform InfoSec behaviours, even when they are not being supervised? (COL5)	Never; Very Little; Little; Somewhat; Much; Very much; A great deal	Brondino, Pasini and Costa (2013); Chan, Woon and Kankanhalli (2005); Lingard, Cooke and Blismas (2009)

The questions or items were designed to be consistent with those employed by prior studies. The questions which focused on climate perceptions of direct supervisors addressed the supervisors' behaviours such as updating respondents on InfoSec procedures or discussing InfoSec matters with respondents and their colleagues (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013). The questions about climate perceptions of colleagues' InfoSec behaviours aimed at measuring respondents' perceived intensity of such behaviours which involve discussing InfoSec issues or taking InfoSec seriously even when rushing work deadlines.

While Chan, Woon and Kankanhalli (2005) named the construct of colleagues' InfoSec behaviours as 'co-worker socialisation', I decided to name this construct 'perception of colleagues' InfoSec behaviours' as this term describes more accurately the items which belong to the theoretical construct. Chan, Woon and Kankanhalli (2005) used the term 'co-worker socialisation' as they conceptualised the InfoSec-related socialisation as a perceived InfoSec behaviour which they defined as the 'daily interactions that the individual has with co-workers' (Chan, Woon & Kankanhalli 2005, p. 24). In this project, the concept of socialisation was operationalised as networks which represented employees' provisions of instrumental resources, of expressive resources and of InfoSec support. My operationalisation of employees' socialisation refers to the actual provisions of organisational resources that take place between the respondent and their colleagues, rather than the socialisation between other employees perceived by the respondent as a third-party observer.

6.2.4 The Instrumental Theory to Identify Influential InfoSec Champions

To analyse the socialisation and InfoSec influence that were expressed as networks, the project team selected graph theory (Barnes & Harary 1983) as the instrumental theory. We used graph

theory as an instrumental theory to perform two analyses: 1) computing employees' centrality measures in the InfoSec-related networks to identify the influential champions and 2) analysing the relationship between the networks representing employees' socialisation and the InfoSec influence network.

Valente and Davis (1999) recommended the sociometric approach, as facilitated by graph theory (Barnes & Harary 1983), for selecting opinion leaders to support the implementation of changes in a community. The theory about opinion leadership identifies key members who can accelerate the diffusion of ideas based on the nominations that they receive from other community's members (Liu et al. 2017; Valente & Davis 1999). This sociometric approach was applied in empirical researches (e.g., Cross et al. 2006; Gesell, Barkin & Valente 2013; Valente 2012) to select opinion leaders for organisational changes by counting the received nominations and calculating the individuals' centrality measures. Consequently, opinion leadership theory (Valente & Davis 1999) served as the second instrumental theory in this stage, which informed the use of network centrality to select the InfoSec champions.

I planned to perform ERGM as a research method to explore employees' characteristics and interactions that contributed to their InfoSec influence. Performing an ERGM analysis involves specifying and evaluating a model that explains the formation of network ties. With the adoption of ERGM method I sought to statistically determine the characteristics and interactions that made an employee in TTT be nominated by other employees as their InfoSec influencers. Moreover, the use of ERGM enabled such statistical analysis while accounting for the unique structural features of the focal networks. This produced findings about employees' influential characteristics and interactions that are relevant to TTT context.

Figure 6.2 summarises the theoretical model of this stage, which described the relationships between the variables to be analysed with the ERGM method. Employees' socialisation was represented by the three networks of their provisions of instrumental resources, expressive resources and InfoSec support. Consistent with the theory of social power bases (Raven 2008), I assumed the providers of these resources would exert influence over the receivers by demonstrating their social powers. Thus, the networks of provisions of resources would co-occur with the InfoSec influence network. Finally, employees' background characteristics such as age, gender and seniority were included as control variables which impacted InfoSec influence.

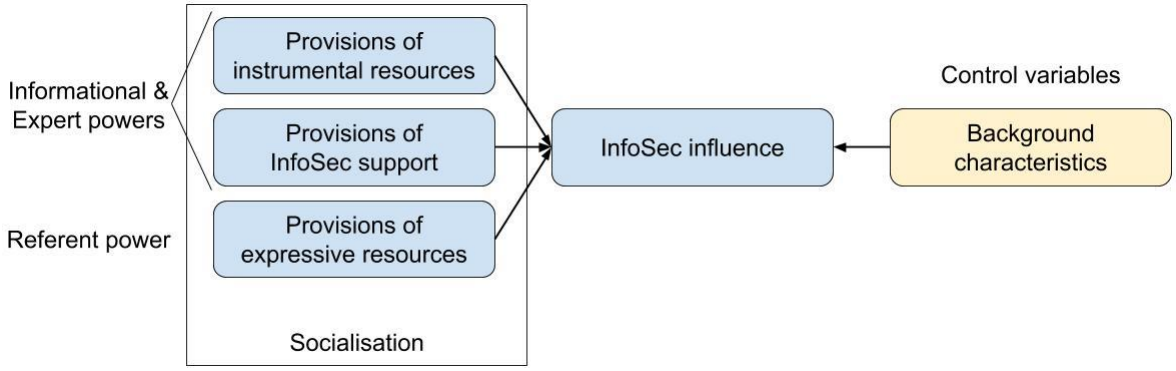


Figure 6.2. Theoretical Model of the Action Planning Stage

The detailed action plan of this stage is as follows. First, the project team would launch the survey to collect data about employees' perceptions of InfoSec climate, their nominated providers of instrumental resources, expressive resources and InfoSec support and the InfoSec influencers that they recognised in the workplace. Second, I would perform analyses on the captured networks and employees' background characteristics to 1) assess the current networks of socialisation at TTT and 2) identify influential InfoSec champions. These analyses would be the descriptive analysis to examine the networks' structural features and the ERGM analysis to determine the factors that enabled an employee to exert InfoSec influence over another employee. The selection of champions would be based on the findings derived from the ERGM analysis and on employees' network centrality.

6.3 Action Taking

6.3.1 Data Collection

The questions summarised in Table 6.1 were incorporated into an online questionnaire sent to all TTT's employees in November 2015. The participants were asked to select themselves from a dropdown list containing the names of 311 employees at that time, followed by the request that they nominate a maximum of seven colleagues they interact with as per the asked questions. The number of seven nominations was based on the recommendation about the number of nominees in Asian organisations required for meaningful network analysis (Merluzzi & Burt 2013). To minimise the intrusive nature of the network questionnaire, which asked employees to nominate their social relationships (Borgatti, Everett & Johnson 2013), the General Director sent an email to all employees which clearly explained that employees' responses would be used strictly for research purposes. Further, top management would not have access to the collected responses.

The project team retrieved responses from 264 of 311 employees (85%). The collected networks and background information were used for the ERGM analysis to determine the contributing characteristics of InfoSec influence and to visualise and evaluate the networks. The demographics of these 264 employees were presented as follows. The number of male employees is higher than the number of female employees (see Figure 6.3). Of these employees, 231 were operational staff, 31 were managers and two were directors (see Figure 6.4).

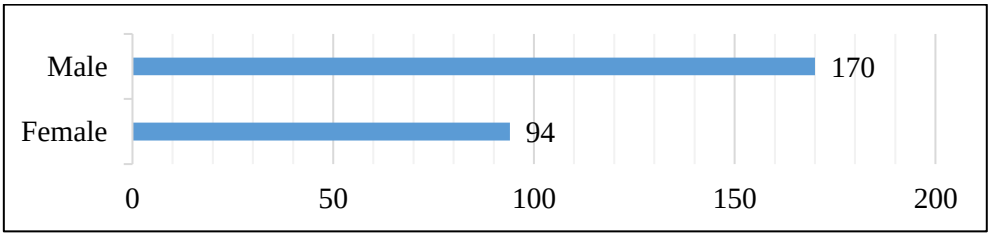


Figure 6.3. Gender Ratio (n = 264)

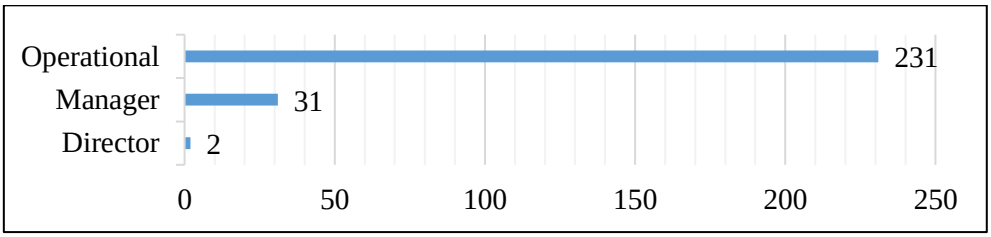


Figure 6.4. Seniority Ratio (n = 264)

Figure 6.5 summarises the age distribution of the 264 employees, showing that a majority of the respondents were relatively young. The average age of the sample was about 41 years old with a standard deviation of 11.63. The four youngest respondents were 22 years old and the oldest respondent was 62.

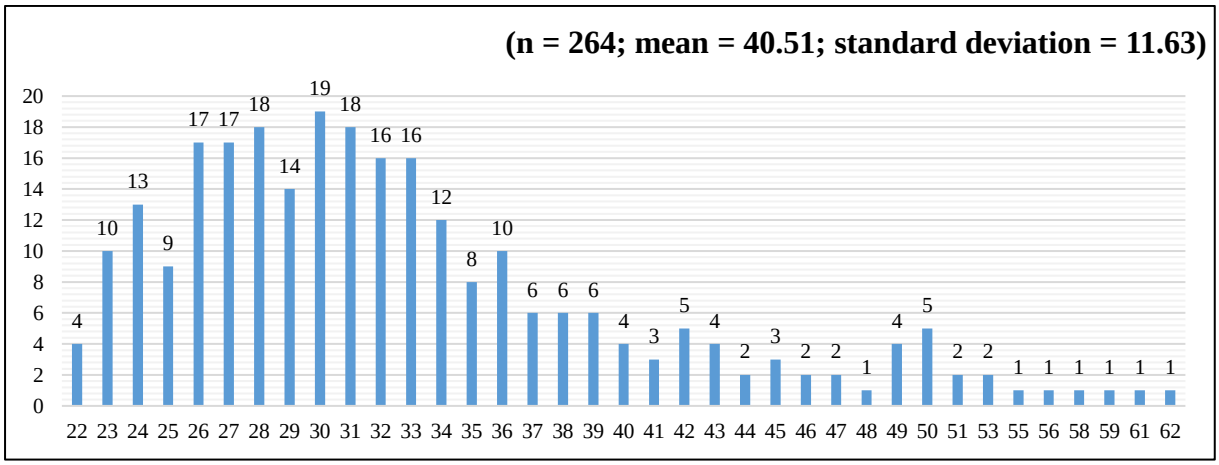


Figure 6.5. Age Distribution (n = 264)

Figure 6.6 presents the distribution of tenure in the sample. Similar to the age distribution, the tenure data indicates that many employees had only recently joined TTT. This tenure distribution reflects the nature of the construction industry in Vietnam where the turnover rate is high and employees frequently change jobs. The average tenure in TTT is about 11 years with a standard deviation of 6.92. There were 65 employees who had just joined TTT (i.e., zero years tenure) and the two most senior employees had been with TTT for 23 years.

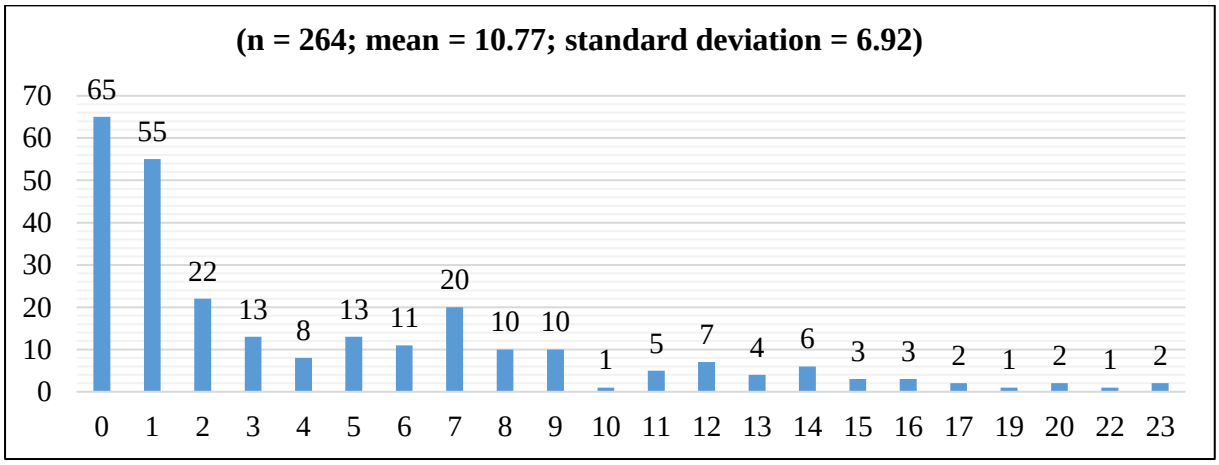


Figure 6.6. Tenure Distribution (n = 264)

Figure 6.7 presents the number of employees per department in the collected sample. The sample comprised 20 departments, with the construction department having the highest number of respondents (82), followed by the architect, factory and project management departments. This distribution is good reflection of TTT's population, reinforcing that the analysis of this sample can be considered meaningful and representative for the larger population.

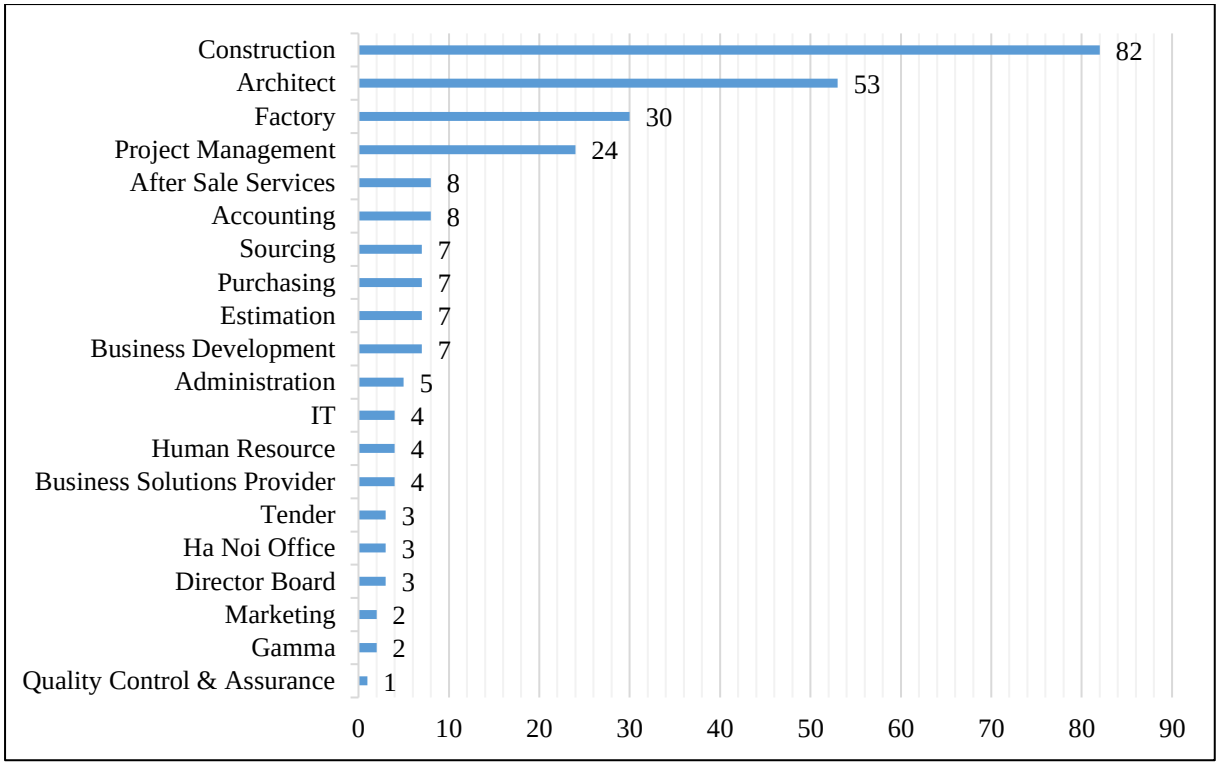


Figure 6.7. Number of Employees per Department (n = 264)

6.3.2 Descriptive Analysis

This section visualises and analyses four networks that represent the provisions of instrumental and expressive resources, InfoSec support and InfoSec influence. The analysis of these visualisations focused on the characteristics of the nodes and their clusters which were formed by their provisions of resources and InfoSec influence represented by network ties.

6.3.2.1 Node's centrality and clusters

To characterise the prominence of a node, I calculated the out-degree centrality i.e., the sum of the outgoing ties sent from a node to its direct neighbours (Borgatti, Everett & Johnson 2013). Since the networks in this research represented the outflows of resources, or the behaviour about sending resources from one individual to another, out-degrees was calculated to evaluate a node's direct provisions of resources or influence. The calculation was performed by using the software UCINET (Borgatti, Everett & Freeman 2002) for descriptive SNA.

After computing out-degree centrality of the nodes, I visualised these measures where larger nodes with larger labels represented having more direct influence and provisions of resources in their networks. The nodes representing employees were coloured according to their department membership. Additionally, the colours of the ties reflect the sources they are sent

from. By using this colouring system, the project team could detect prominent nodes and their areas of influence.

Analysing the nodes' centrality and clusters in the visualisations revealed patterns that reflected the work operations and influences in TTT. The instrumental network (Figure 6.8) shows that employees sought work advice and organisational updates from colleagues who work in the same department. There were distinctive clusters of employees in the estimation, after sale services, accounting and factory departments who actively interacted with each other but not with employees outside their department. There was one large cluster that comprised employees from the project management and construction departments. This clustering pattern was consistent with operations in TTT where these two departments closely collaborated to manage and deliver projects. Similarly, the project team observed the after sale services, business development and estimation departments were tied to each other. In practice, these departments' duties focused on providing customer services to both potential and current clients pre-contract and post-project. Overall, these clusters suggested that employees chose to give instrumental resources to and seek them from other employees whose work was relevant to them.

The project team also identified the prominent employees in this network of the provision of instrumental resources based on the nodes' out-degrees. There were several employees within each cluster who gave work advice and/or organisational updates to many others. Of these, node #9 of the administration department and node #144 of the HR department stood out in the network due to their high out-degrees. A separate analysis of the 'give organisational updates' network confirmed that these nodes were nominated by many other employees for being the central sources of information about the company's policies and work procedures.

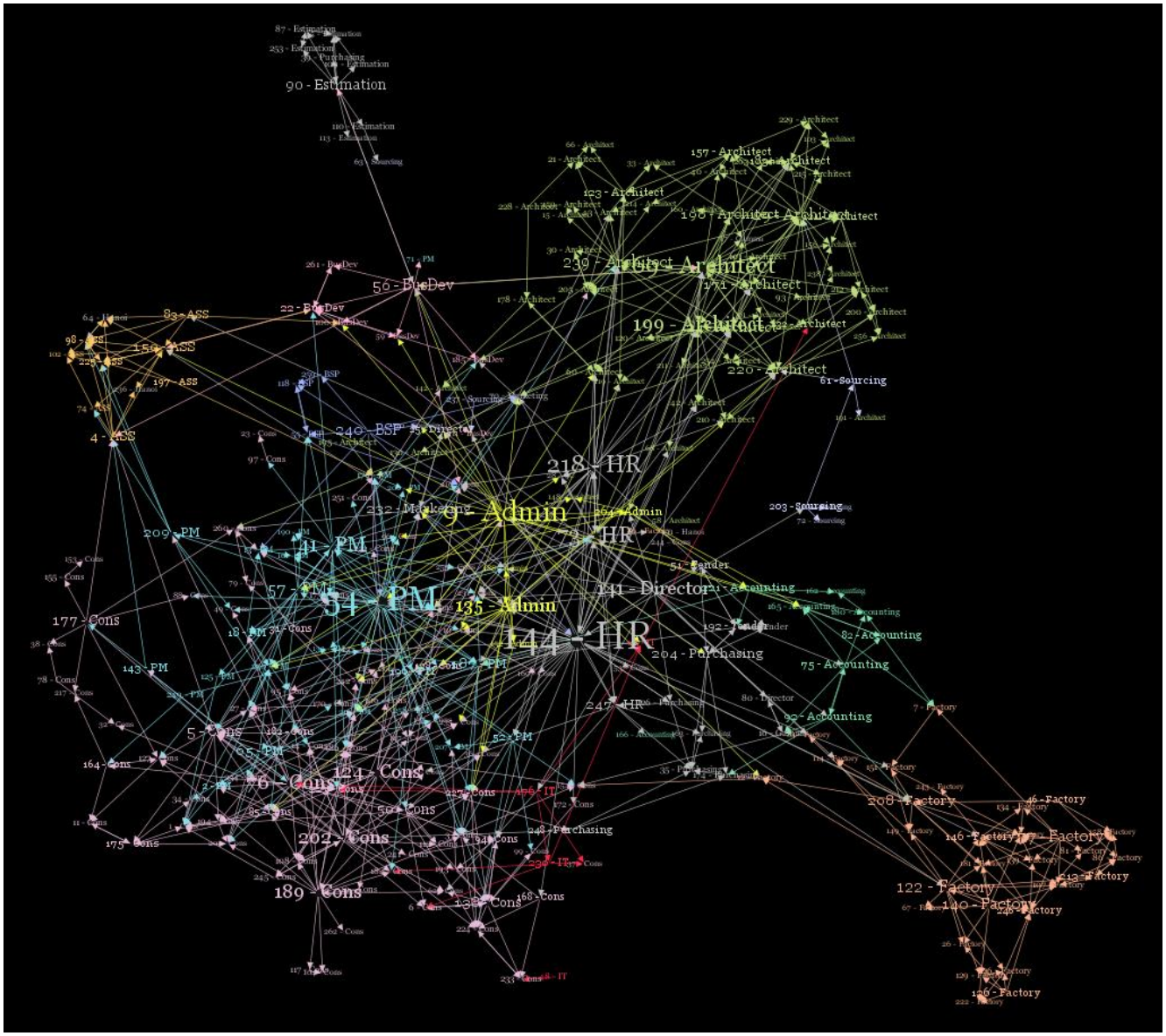


Figure 6.8. Instrumental Network

The expressive network (Figure 6.9) resembled the instrumental network (Figure 6.8). There were some interesting patterns which depicted the informal interactions between employees at TTT. While the number of clusters remained similar to the instrumental provision network, the positions of the employees in the project management department were different. Rather than forming a large cluster and mixing with the construction department, the project management employees were found to be separated into two subclusters (i.e., led by nodes #2 and #54). These clustering patterns showed that employees in the construction department could easily seek personal advice and trust their colleagues in the same department for their expertise. In contrast, there were two social cliques in the project management and construction departments, and members of these cliques socialised with different peers. The project

management and construction employees in the clique led by node #2 tended to exchange expressive resources with those in the factory department. Members of the clique led by node #54 chose to socialise with employees of smaller departments such as after sale services, administration and HR.

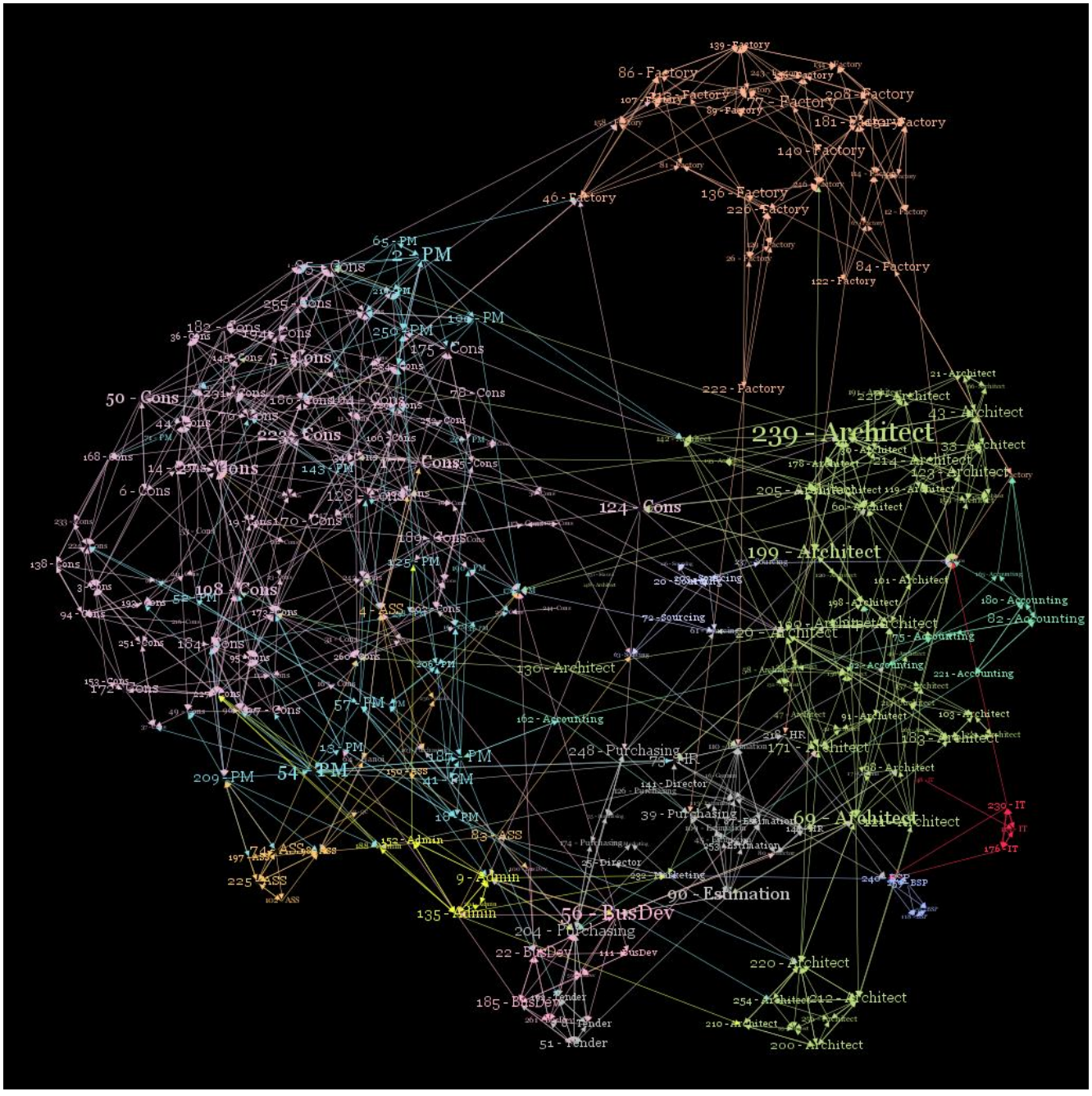
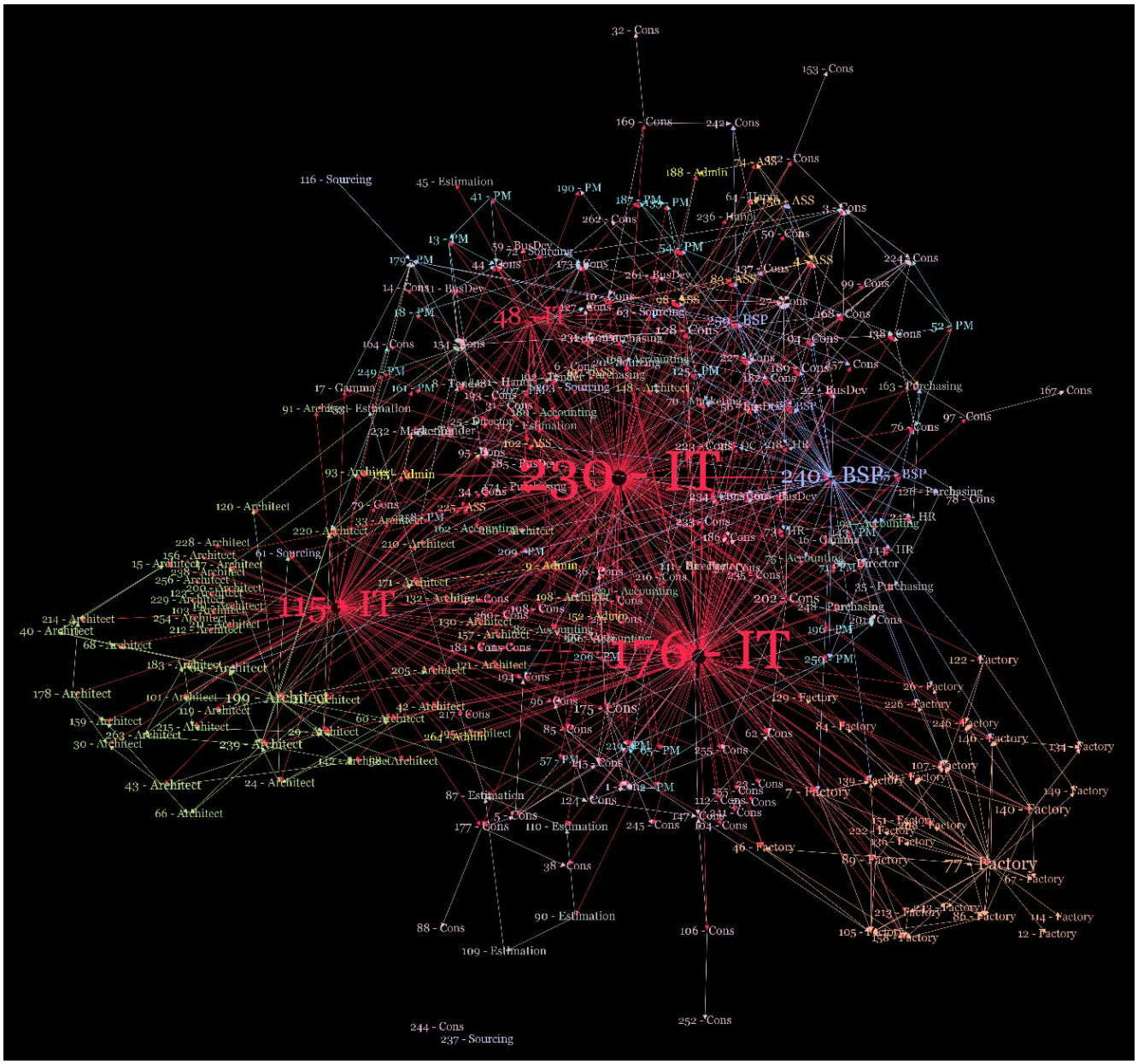


Figure 6.9. Expressive Network

Another interesting pattern was the relationships between the accounting department and the architect department. While employees in the accounting department liaised with the factory department in the instrumental network, they tended to exchange personal advice and trust with

those in the architect department. A common feature of the two networks (see Figures 6.8 and 6.9) was the distinctive clusters of employees in the factory and architect departments who consistently interacted with each other. Their consistent interactions can be explained by the fact that employees in these departments worked in their own buildings away from the headquarters where other departments were located. Therefore, the physical proximity facilitated their tendency of socialisation.


48 - IT
230 - IT
240 - BSP
115 - IT
176 - IT
199 - Architect
202 - Cons
175 - Cons
77 - Factory
32 - Cons
153 - Cons
169 - Cons
242 - Cons
116 - Sourcing
45 - Estimation
188 - Admin
190 - PM
41 - PM
262 - Cons
3 - Cons
13 - PM
59 - BusDev
54 - PM
44 - Cons
224 - Cons
99 - Cons
14 - Cons
52 - PM
18 - PM
63 - Sourcing
128 - Cons
138 - Cons
164 - Cons
249 - PM
17 - Gamma
161 - PM
163 - Purchasing
167 - Cons
91 - Architect
97 - Cons
76 - Cons
232 - Marketing
93 - Architect
120 - Architect
79 - Cons
78 - Cons
61 - Sourcing
15 - Architect
214 - Architect
40 - Architect
68 - Architect
178 - Architect
101 - Architect
30 - Architect
43 - Architect
24 - Architect
66 - Architect
239 - Architect
29 - Architect
42 - Architect
60 - Architect
119 - Architect
159 - Architect
263 - Architect
215 - Architect
256 - Architect
228 - Architect
156 - Architect
254 - Architect
212 - Architect
183 - Architect
205 - Architect
217 - Cons
264 - Admin
142 - Architect
Architect
171 - Architect
132 - Architect
Cons
157 - Architect
184 - Cons
Cons
194 - Cons
206 - PM
250 - PM
122 - Factory
26 - Factory
120 - Factory
226 - Factory
246 - Factory
140 - Factory
134 - Factory
107 - Factory
139 - Factory
149 - Factory
140 - Factory
151 - Factory
222 - Factory
136 - Factory
46 - Factory
89 - Factory
67 - Factory
213 - Factory
80 - Factory
114 - Factory
12 - Factory
105 - Factory
58 - Factory
84 - Factory
62 - Cons
85 - Cons
96 - Cons
87 - Estimation
124 - Cons
5 - Cons
177 - Cons
110 - Estimation
245 - Cons
38 - Cons
90 - Estimation
88 - Cons
109 - Estimation
106 - Cons
244 - Cons
237 - Sourcing
252 - Cons
74 - Admin
61 - Temp
236 - Admin
59 - BusDev
Sourcing
261 - BusDev
137 - Cons
89 - ASS
99 - Cons
10 - Cons
95 - ASS
27 - Cons
63 - Sourcing
128 - Cons
Purchasing
234 - Cons
168 - Accounting
227 - Cons
125 - PM
87 - Cons
169 - Cons
157 - Cons
Tender
Purchasing
193 - Cons
Sourcing
118 - Architect
22 - BusDev
163 - Purchasing
31 - Cons
181 - Accounting
25 - Director
Estimation
102 - ASS
95 - Cons
185 - Purchasing
34 - Cons
225 - ASS
33 - Architect
162 - Accounting
Architect
210 - Architect
209 - PM
9 - Admin
36 - Cons
216 - Cons
111 - Director
Cons
Accounting
71 - PM
Director
16 - Gamma
HR
85 - Purchasing
248 - Purchasing
75 - Cons
196 - PM
Cons
Cons
Accounting
Cons
198 - Architect
Cons
260 - Cons
152 - Admin
130 - Architect
Accounting
Cons
Cons
Cons

support. The IT department looked after the company's technological infrastructures while the BSP department focused on delivering training and implementation for information systems (e.g., enterprise resource planning and customer relationship management systems). In Figure 6.10, the project team also observed that IT and BSP employees had their own areas of providing InfoSec support, such as employees #240, #230 and #48 nominated by departments in the headquarters and #176 and #115 nominated by the factory and architect departments respectively.

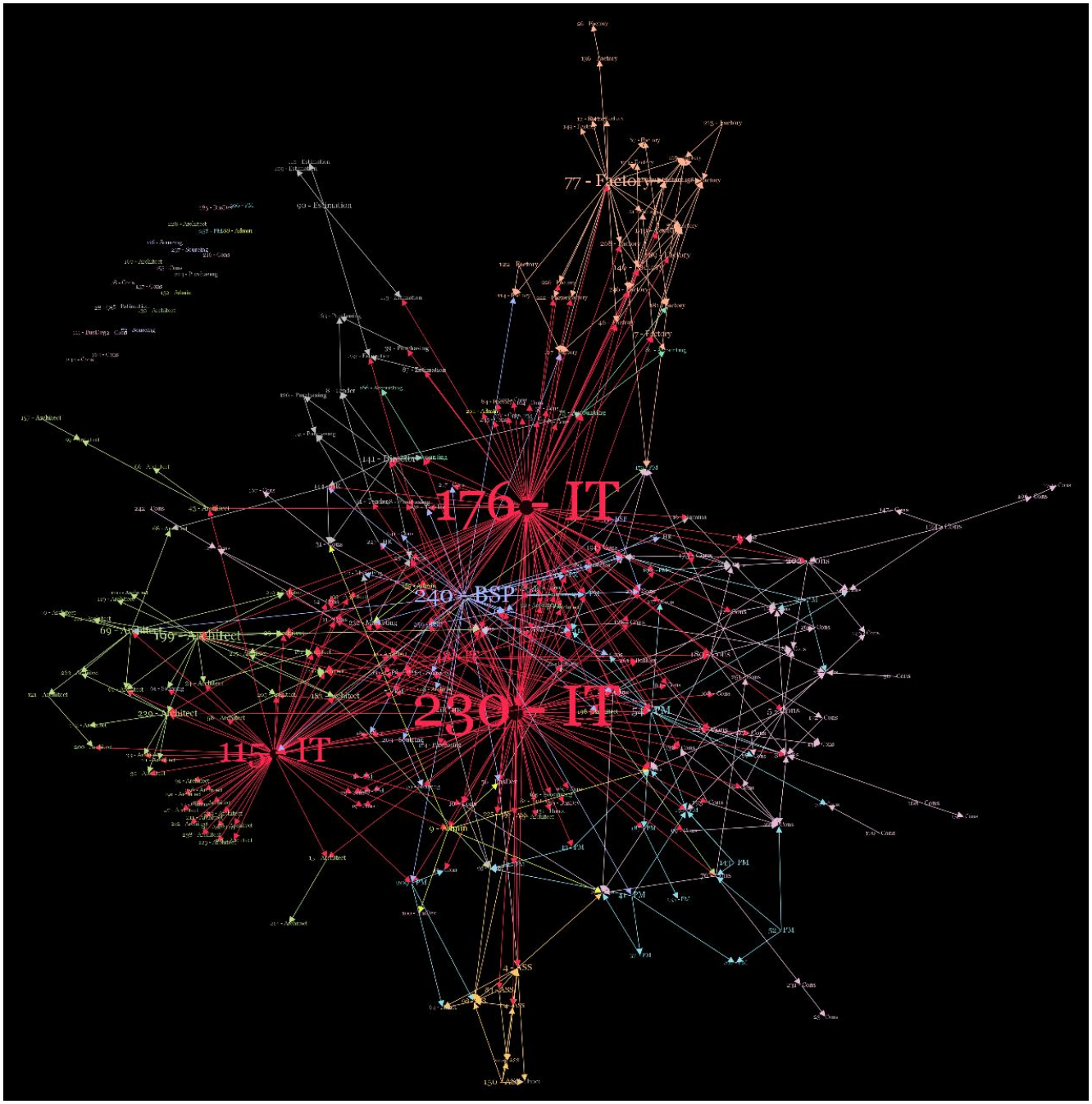


Figure 6.11. InfoSec Influence Network

Figure 6.11 presents the visualisation of the InfoSec influence network which resembled the visualised InfoSec support network. Employees of the IT and BSP departments held influential roles in this network. They also attracted nominations from three distinctive areas including headquarters and the factory and architect departments. The high similarity between the InfoSec influence network and the InfoSec support network suggested that these two types of interactions would be more likely to co-occur with each other.

6.3.2.2 Network statistics

I calculated network statistics (summarised in Table 6.3) to quantitatively analyse the networks' structural features. This analysis allowed a more accurate comparison of the features across the networks.

Table 6.3. Network Statistics

	Instrumental network	**Expressive network**	**InfoSec support network**	**InfoSec influence network**
Density (the ratio of existing ties over all possible ties)	0.011	0.014	0.012	0.008
Average degree (the average number of ties per node)	3.023	3.727	3.098	2.045
Out-degree centralisation (the variation in the out-degree centrality scores among all nodes)	0.149	0.051	0.610	0.351
Reciprocity (the ratio of reciprocated ties)	0.098	0.348	0.010	0.007
Transitivity (the extent to which the nodes tend to cluster together)	0.188	0.211	0.500	0.305

Density characterises the connectedness of the whole network (Borgatti, Everett & Johnson 2013; Hanneman & Riddle 2005). Density is calculated by taking the ratio between the observed ties and the maximum number of all possible ties. This measure has meaningful implications in practice. For example, a densely connected communication network is desirable for information to effectively reach all the nodes (Rowley 1997). Conversely, thinner networks with more structural holes grant the nodes access to more unique information and increase each node's bargaining power (Halgin & Borgatti 2012). In the context of diffusing information, dense networks facilitate the spread of innovative ideas and norms resulting in similar behaviours of nodes in the network (Gesell, Barkin & Valente 2013; Rowley 1997).

Of the four networks, the expressive network had the largest density. This meant that providing personal advice and trusting other employees for their expertise were more common than other forms of socialisation in TTT. In contrast, the InfoSec influence network had the lowest density, meaning that such influence rarely occurred between random pairs of employees. Even though networks are considered as dense or sparse differently depending on the subjective context and expert judgments, a network having a density value of 0.15 or above can be considered as densely connected (Gesell, Barkin & Valente 2013). In this case, even the most connected expressive provision network only had a density value of 0.014, indicating that the operations in TTT were rather silo-based.

In terms of average degree (i.e., the average number of ties per node), the expressive network had the highest value. This indicated that the provision of personal advice and trust in expertise were the most common among the four examined interactions. Moreover, an employee provided personal advice and/or trust with at least three colleagues on average. The InfoSec influence network had the lowest value of average degree, which suggested that InfoSec influence was rare. These findings were consistent with the network density values discussed above.

Out-degree centralisation describes the variation in the out-degrees within a network (Borgatti, Everett & Johnson 2013). Evaluating out-degree centralisation informs the hierarchical level of a network, since a high value of out-degree centralisation indicates a large gap between the lowest and the highest number of outgoing ties possessed by the nodes (Ahuja & Carley 1998). In line with the visual analysis, the InfoSec support and InfoSec influence networks had out-degree centralisation values (0.610 and 0.351 respectively) much higher than those of the instrumental and expressive networks. The hierarchical structures in these InfoSec-related networks could be observed in the network visualisations (Figures 6.8 and 6.9). There were only a handful of IT and BSP employees who received many nominations from other employees for being capable of exuding InfoSec influence and InfoSec support.

Reciprocity reflects the tendency of a node to return a tie to another connected node (Borgatti, Everett & Johnson 2013). High reciprocity in an information sharing or learning context informs the tendency of members actively exchanging ideas, whereas low reciprocity implies that there are many one-way communications. As the expressive network was the most densely connected it was not surprising to see that it also had the highest reciprocity value (0.348). In contrast, the InfoSec support and InfoSec influence networks had the lowest reciprocity values,

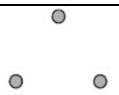
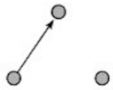
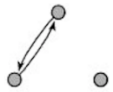
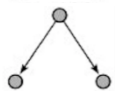
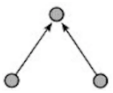
which indicated that the provision of InfoSec support and InfoSec influence tended to be unidirectional.

Transitivity reflects the tendency of the nodes to cluster together, which follows the saying 'friends of my friends are my friends' (Borgatti, Everett & Johnson 2013). Another interpretation of transitivity is that it reflects the tendency of actor A to establish a connection with actor C if both are connected with an intermediate actor B (Borgatti, Everett & Johnson 2013). As shown in Table 6.3, the InfoSec support and InfoSec influence networks had the highest values for transitivity, which was understandable since most of the nodes tended to cluster around the IT and BSP staff.

6.3.2.3 Triad census

Triad census is a concept related to network transitivity. To elaborate on triad census, I examined the triadic configurations or the structures of a three-node set (i.e., a triad) (Hanneman & Riddle 2005). The three types of triadic structures of the four examined networks—local, transitive and intransitive—are summarised in Tables 6.4, 6.5 and 6.6 respectively. Each triadic configuration is assigned a unique code such as 003, 012 and 102, following the Mutual-Asymmetric-Nulls naming convention (Holland & Leinhardt 1976). The statistics of each configuration report the number of times the configuration appeared in each of the four networks.

Table 6.4. Local Triadic Configurations of the Four Examined Networks

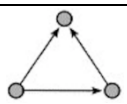
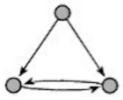
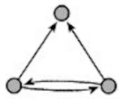
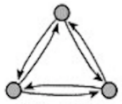
Triadic configuration	Illustration	Instrumental network	Expressive network	InfoSec support network	InfoSec influence network
003		2,840,207	2,824,223	2,852,506	2,902,844
012		175,241	159,951	145,350	116,933
102		9,608	42,784	813	385
021D		3,633	870	30,934	10,394
021U		772	916	709	415

Local structures are the configurations of three nodes that describe basic patterns of the network, such as '003' (a null triad), '012' (one tie among three nodes) and '102' (a reciprocal

dyad). All networks shared similar amounts of ‘003’ and ‘012’ configurations. The expressive network had the highest number of reciprocity between two nodes (i.e., ‘102’ configuration) followed by the instrumental network.

The InfoSec-related networks were rarely reciprocal. In other words, the provision of InfoSec support and InfoSec influence were both mostly unidirectional. This finding was consistent with these networks’ reciprocity values reported in the previous section. The configuration coded ‘021D’ describes triadic dominancy, where there is one node sending out ties to the other two while not receiving any ties in return. It was interesting to observe that the InfoSec support and InfoSec influence networks had more of this structure than the instrumental and expressive networks. This observation matched these networks’ high out-degree centralisation values. The InfoSec influence network had the smallest number of ‘021U’ coded configuration, indicating that an employee hardly had their InfoSec practices influenced by two people at the same time compared to other networks.

Table 6.5. Transitive Triadic Configurations of the Four Examined Networks

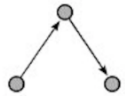
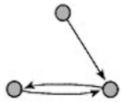
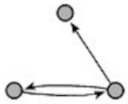
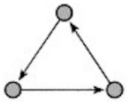
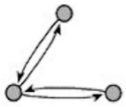
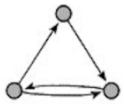
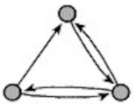
Triadic configuration	Illustration	Instrumental network	Expressive network	InfoSec support network	InfoSec influence network
030T		307	190	594	179
120D		32	58	7	0
120U		35	79	114	55
300		0	20	0	0

There are four types of transitive configurations, as shown in Table 6.5, where resources flow among all members of the same triad. The configuration coded ‘030T’ represents triad closure, or the tendency of a node to send a direct tie to another one that shares a common node in between, which closes a triad. This configuration reflects a hierarchy in a triad as there is one member that only sends out ties to the other two. The InfoSec support network had the highest number of this configuration which reflected its transitive and hierarchical nature.

The configuration coded ‘120D’ also reflects a hierarchy within a triad, but there is an exchange of resources between the two receivers. The InfoSec-related networks ranked quite low in terms

of having this configuration, which further reinforced their hierarchical nature and that reciprocal ties only occurred between the receivers. These InfoSec-related networks ranked higher in terms of the configuration coded '120U', which referred to the situation where two employees, such as IT or BSP employees, exchanged InfoSec advice and troubleshooting support while providing these resources to a third employee. The configuration coded '300' describes complete transitivity; only the instrumental network and especially the expressive network had this configuration. It showed a situation where all three members shared instrumental and/or expressive resources with each other.

Table 6.6. Intransitive Triadic Configurations of the Four Examined Networks

Triadic configuration	Illustration	Instrumental network	Expressive network	InfoSec support network	InfoSec influence network
021C		1,510	1,159	723	575
111D		128	619	16	12
111U		355	725	98	72
030C		2	8	0	0
201		17	158	0	0
120C		8	47	0	0
210		9	57	0	0

Triadic configurations are intransitive due to having a certain degree of inequality in their connections, where actor A fails to establish a connection with actor C via actor B (Hanneman & Riddle 2005). The InfoSec-related networks only had the intransitive configurations coded '021C', '111D' and '111U'. The configuration coded '021C' describes a two-path structure, or the tendency of a node to maintain indirect connections to another one via an intermediate node. Since the InfoSec support network had a high amount of the triad closure configuration, as previously discussed, its small number of two-path configurations confirmed the transitive nature of this network. Since the InfoSec support and InfoSec influence networks also had low amounts of the intransitive configurations coded '111D' and '111U', these networks would be

highly transitive. The high transitivity implied that employees formed clusters by providing each other with InfoSec support and exerting InfoSec influence. Further, the project team could make use of such transitive nature to facilitate the provision of InfoSec support and InfoSec influence.

6.3.3 Exponential Random Graph Modelling

After examining the descriptive characteristics of the networks, I conducted ERGM to determine employees' characteristics and socialisation that contributed to InfoSec influence and to identify the influential InfoSec champions. I performed the ERGM analysis by following the recommendations of Hunter et al. (2008), Goodreau et al. (2008) and Desmarais and Cranmer (2012) in regard to ensuring the robust analysis of exponential random graph models. Details about the ERGM method, its estimation process and the raw results of the ERGM analysis are in Appendix D.

Three exponential random graph models were specified and analysed—Model 1, Model 2 and Model 3. Model 1 only accounted for the background characteristics of employees and their impacts on the likelihood of occurrence of InfoSec influence ties. Model 2 extended Model 1 by evaluating the impacts of not only employees' background characteristics, but also of their socialisation (i.e., the provisions of instrumental resources, expressive resources and InfoSec support between employees). Model 3 extended Models 1 and 2 by evaluating the impacts of both employees' background characteristics and socialisation, while accounting for the unique structural characteristics of the InfoSec influence network such as reciprocity and transitivity.

Table 6.7 summarises the results of the three mentioned exponential random graph models which indicated the impacts of employees' characteristics (e.g., age, gender and seniority) and socialisation (e.g., provision of InfoSec support) on the likelihood of the occurrence of InfoSec influence ties (i.e., the likelihood that an employee would exert InfoSec influence over another employee). The results also indicated the structural tendencies of the InfoSec influence network, which were reciprocity, in- and out-degree variations of nodes and transitivity.

Table 6.7. ERGM Results

Effect	Model 1	Model 2	Model 3
InfoSec influence between random employees	–2.96*** (0.40)	–4.66*** (0.57)	–4.17*** (0.56)
Influencer is female	–1.27*** (0.12)	–0.83*** (0.18)	–0.36** (0.15)
Influenced employee is female	–0.24** (0.12)	–0.16 (0.16)	–0.15 (0.16)
Employees have the same gender	0.02 (0.12)	–0.05 (0.16)	–0.03 (0.16)
Employees have the same department	1.10*** (0.09)	0.47*** (0.15)	0.76*** (0.15)
Influencer's age	–0.09*** (0.01)	–0.07*** (0.02)	–0.02 (0.01)
Influenced employee's age	0.001 (0.01)	0.02 (0.01)	0.01 (0.01)
Employees have different ages	–0.01 (0.01)	–0.02 (0.01)	–0.01 (0.01)
Employees have the same seniority	0.06 (0.13)	–0.27 (0.18)	–0.18 (0.19)
Influencer is a manager	1.48*** (0.15)	0.72*** (0.20)	0.31 (0.19)
Influencer is a director	1.51*** (0.41)	1.88*** (0.46)	1.35*** (0.30)
Influenced employee is a manager	0.30** (0.14)	–0.03 (0.19)	–0.03 (0.19)
Influenced employee is a director	0.54 (0.47)	0.24 (0.64)	0.38 (0.61)
Influencer's tenure	0.23*** (0.02)	0.16*** (0.02)	0.06*** (0.02)
Influenced employees's tenure	–0.01 (0.01)	–0.03 (0.02)	–0.03** (0.02)
Employees have different tenures	–0.08*** (0.01)	–0.05*** (0.02)	–0.04** (0.02)
Employees provide each other with instrumental resources		1.98*** (0.21)	1.93*** (0.19)
Employees provide each other with expressive resources		0.91*** (0.22)	1.14*** (0.21)
Employees provide each other with InfoSec support		5.33*** (0.12)	4.31*** (0.14)
Variation in out-degrees			–3.16*** (0.39)
Variation in in-degrees			–1.03*** (0.38)
Triad closure (network's tendency of being transitive)			0.50*** (0.10)
Two-path (tendency to maintain indirect influence)			–0.07*** (0.03)
Reciprocity (tendency to reciprocate influence)			–1.74 (1.19)
Control for the number of 'sinks' (out-degrees = 0)			–1.10*** (0.39)
Control for the number of 'sources' (in-degrees = 0)			–0.95** (0.44)
Control for the number of 'isolated' employees			–0.19 (0.39)
Akaike Information Criterion	5438	2763	2609
Bayesian Information Criterion	5584	2937	2856

Note: Statistically significant results are bolded; results' standard errors are in brackets; **p < 0.05; ***p < 0.01.

The results in Table 6.7 are in log-odds and can be converted to probabilities in percentage by using the formula below:

$$\text{probability} = \frac{\exp(\text{log-odds})}{1 + \exp(\text{log-odds})}$$

Each of the three examined ERGM models had a baseline probability for an employee to influence another employee's InfoSec practices when no specific background characteristics or forms of socialisation were considered (i.e., an InfoSec influence between two random employees). By using the provided formula, the calculated baseline probabilities that employees would exert InfoSec influence in random pairs were 4.93 per cent (Model 1), 0.93 per cent (Model 2) and 1.52 per cent (Model 3). Overall, these low probabilities indicated that it was rare for random employees to influence each other's InfoSec behaviours which matched with the descriptive analysis above.

When there was a specific characteristic (e.g., the influencer was female or the influenced employee was a manager) or a provision of resources between the employees (e.g., the influencer provided the influenced employee with InfoSec support) the baseline probability would change accordingly. Table 6.8 shows some scenarios and uses the results from Model 3 to calculate the probabilities for employees having various characteristics to exert InfoSec influence over each other. For example, when both employees worked in the same department the probability that an InfoSec influence tie occurred between these employees would increase from 1.52 per cent to 3.2 per cent (Model 3). If two employees had the same department membership and one of them gave InfoSec support to the other, then the total log-odds of InfoSec influence tie's occurrence between them would increase from –4.17 to 0.9 (–4.17 + 0.76 + 4.31) which corresponded to an increase in probabilities from 1.52 per cent to 71.09 per cent.

Table 6.8. Scenarios and Probabilities of Exerting InfoSec Influence

Scenario	Log-odds	Probability
Random employees exerted InfoSec influence over each other	–4.17	1.52%
Employees in the same departments exerted InfoSec influence over each other	(–4.17 + 0.76) = –3.41	3.20%
Employees in the same departments exerted InfoSec influence over each other, and these employees also provided each other with InfoSec support	(–4.17 + 0.76 + 4.31) = 0.9	71.09%

Some effects of employees' background characteristics (e.g., department manager status of the influencer and influenced employee) became non-significant in Model 2 and/or Model 3 when they were evaluated together with the effects of employees' socialisation. An explanation for this phenomenon was that these effects (e.g., being a department manager) became less important in terms of creating InfoSec influence ties when the socialisation took place.

The project team considered the effects that remained significant in all three models as critical selection criteria for influential champions. The effects that remained significant in both Models 1 and 2 could also be considered when selecting potential InfoSec champions. Effects that were only significant in Model 1 (e.g., gender of the influenced employee) and effects that caused minor changes in the probabilities of occurrence of InfoSec influence ties (e.g., tenure of the influencer, which caused a slight increase from 0.94% to 1.1%) were considered as trivial and unsuitable to be selection criteria. The results in Table 6.7 are elaborated on below.

6.3.3.1 Effects of background characteristics on InfoSec influence

I evaluated the impacts of five background characteristics of an employee—gender, age, department membership, seniority and tenure—on the occurrence of InfoSec influence ties. The evaluated effects focused on the characteristics of the influencers, influenced employees and pairs of employees (i.e., whether the pairs had similar or different characteristics). The results indicated that female employees were less likely than male employees to influence and be influenced by other employees. The significant and negative effects of being a female influencer on InfoSec influence were consistent across the three models, whereas the effect of the influenced employees being female was only significant in Model 1. Having the same gender was not found to affect InfoSec influence nor was having different ages. Older employees were less likely to influence other employees' InfoSec behaviours. Nonetheless, the effect of age on InfoSec influence was ignorable, which caused minor changes of –0.41 per cent (Model 1) and –0.07 per cent (Model 2).

Employees with long tenures had a higher chance to exert InfoSec influence over other employees, as shown in the consistently significant and positive log-odds of 0.23 (Model 1), 0.16 (Model 2) and 0.06 (Model 3). However, two employees having similar tenures would be less likely to influence each other's InfoSec behaviours. These findings indicated the positive impact of tenure-based hierarchy on the occurrence of InfoSec influence ties. The effect of tenure on InfoSec influence over the influenced employees only achieved significance in

Model 3 which included structural effects such as reciprocity and transitivity. This indicated that tenure's effect of the influenced employees became important to InfoSec influence only when the InfoSec influence network's structural characteristics were considered.

Department membership and seniority greatly increased the occurrence of InfoSec influence ties. Employees who worked in the same department doubled the chance of influencing each other's InfoSec behaviours from a baseline probability of 1.52 per cent to 3.2 per cent (Model 3). The change in probabilities caused by sharing the same department membership was largest in Model 1 (a change of 8.54%), then dropped to lowest in Model 2 (0.55%) and increased in Model 3 (1.68%). The effect of sharing department membership decreased when employees' socialisation was examined in Models 2 and 3. When information about structural characteristics of the InfoSec influence network were accounted for in Model 3, such as transitivity or the network's clustering tendency, having the same department membership became more important in determining the occurrence of InfoSec influence ties, explaining the increase in the change of probabilities. This was consistent with the analysis of InfoSec influence network (see Figure 6.11) where clusters of employees of the same departments could be visually identified.

Being a department manager or director also enabled an employee to influence other employees' InfoSec behaviours. It was worth highlighting that only the effect of being a director remained significant across the three models, even when the effects of employees' provisions of resources were examined in Model 3. This indicated that the directors in TTT had a strong influence over other employees' InfoSec behaviours, whereas the impact of being department manager on InfoSec influence was negated by those of the provisions of resources.

6.3.3.2 Effects of socialisation on InfoSec influence

Three forms of socialisation (i.e., the provisions of instrumental resources, expressive resources and InfoSec support) were investigated for their impacts on InfoSec influence. The ERGM results indicated that all three of these socialising activities increased the likelihood of InfoSec influence between employees. The provision of InfoSec support, which comprised InfoSec advice and/or troubleshooting support, had the largest impact on InfoSec influence. When an employee gave InfoSec advice and/or troubleshooting support to another employee, the likelihood for that employee to influence the receiver's InfoSec behaviours increased from 0.94 per cent to 66.15 per cent (Model 2) and from 1.52 per cent to 53.49 per cent (Model 3).

The provision of instrumental resources (i.e., giving work advice and/or organisational updates) and the provision of expressive resources (i.e., giving personal advice and/or trusting for expertise) both increased the likelihood of exerting InfoSec influence. We also noticed the changes in impacts of these three socialisation forms on InfoSec influence, of which the impacts of the provisions of instrumental and expressive resources increased, whereas the impact of the provision of InfoSec support decreased. These changes were caused by the inclusion of the InfoSec influence network's structural features in Model 3.

6.3.3.3 Effects of network's structural characteristics on InfoSec influence

Model 3 analysed the structural characteristics of the InfoSec influence network, which focused on its out- and in-degree variations, reciprocity and transitivity. The analysis of these characteristics not only described the network's structure in more detail, but also provided additional explanations for the formation of InfoSec influence ties.

Controlling for employees' background characteristics and socialisation, the results of the InfoSec influence network's out- and in-degree variations were significant and negative in Model 3. Such results indicated homogeneity in employees' tendencies to influence and to be influenced by other employees, or the overall similarities in employees' number of outgoing and incoming InfoSec influence ties.

Transitivity reflects employees' clustering tendency in the network which can also impact the formation of InfoSec influence ties. Model 3 analysed transitivity of the InfoSec influence network which was described by the 'triad closure' and 'two-path' effects. A positive 'triad closure' effect and a negative 'two-path' effect, as shown in the ERGM results, confirmed that the InfoSec influence network was transitive. This also indicated that employees were more likely to receive direct InfoSec influence ties from those who indirectly influenced their InfoSec behaviours via multiple in-between employees. Employees' tendency to close the triads and form InfoSec influence clusters encapsulated the saying 'a friend of my friend is also my friend'.

Model 3 also examined employees' tendency to reciprocate InfoSec influence ties; the result showed that this effect was non-significant. This indicated that there was no pattern with regard to reciprocity in the InfoSec influence network. The result was consistent with the descriptive statistics of the InfoSec influence network (see Table 6.3) which showed that the InfoSec influence network had a low rate of reciprocity.

6.3.4 Calculating Network Centrality of InfoSec Champions

Unlike the background characteristics, such as department membership and seniority, that were observable and readily available to be used as selection criteria for InfoSec champions, identifying potential champions who actively socialised in the networks of provisions of resources required a method to quantitatively measure such socialisation.

Opinion leadership theory, the second instrumental theory in this stage, suggested that champions' positions in the networks can amplify their influence over others (Liu et al. 2017; Valente & Davis 1999). Valente and Davis (1999) and Valente and Pumpuang (2007) proposed several procedures for recruiting opinion leaders, of which allowing all community members to nominate the leaders (i.e., the sociometric procedure) could overcome the shortcomings of the other recruitment procedures. Once the nominations are collected, program teams can calculate the leaders' network centrality measures that reflect their influence in the community (Liu et al. 2017; Valente & Davis 1999). Opinion leadership theory specified that opinion leaders can be selected based on three measures of network centrality—degree centrality, betweenness centrality and closeness centrality (Liu et al. 2017). Degree centrality was defined and analysed in Section 6.3.2. Betweenness centrality counts the number of times a node serves as the bridge that connect pairs of nodes together, and closeness centrality is the sum of the number of hops required for a node to reach all other nodes (Borgatti, Everett & Johnson 2013).

Following opinion leadership theory (Liu et al. 2017; Valente & Davis 1999), I calculated the out-degree centrality of all employees in the networks of provisions of instrumental, expressive, InfoSec support resources and exerting InfoSec influence to measure employees' level of socialisation and their direct influence in these networks. I also considered calculating employees' betweenness centrality and closeness centrality as suggested by Liu et al. (2017); however, Borgatti (2005) discussed the caveats of these two centrality measures—their calculations only account for the shortest paths between the nodes. As such, these measures only reflect the nodes' influence in the networks where all nodes are assumed to know and travel on the shortest paths to reach each other. While this assumption is relevant in situations where following the shortest paths is emphasised (e.g., shipping goods from one location to another location), it is less realistic for transmissions via random paths such as the diffusion of information (Borgatti 2005). The transmissions of advice, trust, troubleshooting support and InfoSec influence among employees would not always follow the shortest paths. Therefore, I

decided that betweenness centrality and closeness centrality would not be appropriate measures for representing employees' influence in the networks examined in this project.

The popularity or influence of a node can also be measured by the nodes' connections with others that are well-connected (Borgatti 2005). An employee who cannot directly influence many employees can still be considered as influential if that employee can influence and leverage their colleagues who are influential. This indirect popularity is measured by Beta centrality which describes employees' indirect influence (Borgatti, Everett & Johnson 2013). Considering employees' Beta centrality is a prudent approach that prevents missing out influential employees while providing more options when selecting champions. Thus, I calculated the Beta centrality of all 264 employees in the networks using the software UCINET (Borgatti, Everett & Freeman 2002) then used these measures together with employees' out-degree centrality to select the influential champions.

6.4 Evaluation

The criteria for selecting champions for the diffusion of InfoSec knowledge were identified through the ERGM analysis. A potential champion would:

- be a director or department manager
- work in the same department of other employees
- have longer tenure than other employees
- have high out-degree centrality and/or Beta centrality in the networks of:
    - provision of instrumental resources (i.e., work advice and/or organisational updates)
    - provision of expressive resources (i.e., personal advice and/or trust for expertise)
    - provision of InfoSec support (i.e., InfoSec advice and InfoSec troubleshooting support)
    - InfoSec influence

Since the abilities to socialise and provide other employees with resources had large impacts on InfoSec influence, I considered these abilities as essential criteria for selecting InfoSec champions. Therefore, I recommended TTT to select employees who possessed high centrality measures in the instrumental, expressive, InfoSec support and InfoSec influence networks to be InfoSec champions.

The ERGM results suggested that being a director could greatly influence other employees' InfoSec behaviours. However, there were not enough directors in TTT who could devote their time to take care of each department's InfoSec environment and to actively diffuse InfoSec knowledge. As a result, the project team concluded that selecting employees who were department managers in the same department with the influenced targets would be a more sensible solution. Although tenure could also improve an employee's ability to exert InfoSec influence, this trait was not considered as a selection criterion due to its small effect on exerting InfoSec influence.

The project team and top management selected 50 champions based on these criteria for the departments in TTT. Each department had one to two champions on average. Large departments such as project management, architect, construction and factory, had six to seven champions. The 50 champions and their characteristics are summarised in Table D.4 in Appendix D.

As part of the evaluation activities, the project team and top management jointly examined the visualisations of the networks of provisions of instrumental, expressive, InfoSec support and InfoSec influence. The top management agreed with the project team that the networks of instrumental and expressive provisions were reflective of TTT's work operations. They also recognised that both InfoSec-related networks (see Figures 6.10 and 6.11) were sparse and thin, and the IT employees and Vice Director of the BSP department stood out in the networks with many connections. Although the architect and factory departments operated in two separate locations, employees in these departments sought InfoSec advice and troubleshooting support from and were influenced by IT employees who worked at headquarters.

It appeared that even for the informal communication of InfoSec matters the structures of the InfoSec support and InfoSec influence networks in TTT followed a 'command-and-control' model, where IT and BSP employees acted as both the formal and informal authority which provided InfoSec-related resources to all employees. The Vice Director of the BSP department and top management commented that although the current command-and-control management model could be useful for maintaining the dissemination of consistent InfoSec advice and troubleshooting support, there would be more disadvantages. This management model relied on a handful of IT and BSP staff and was prone to the risk of cascading failure if erroneous advice were distributed or if one of the IT or BSP staff were to leave TTT. Moreover, the IT

and BSP staff could be overloaded by all the queries and requests concerning InfoSec, which would leave them less time to attend other important duties.

6.5 Reflection

6.5.1 Reflection on the Use of Theory of Social Power Bases

The theory of social power bases (Raven 2008) served as the focal theory of this stage, which suggested the traits and abilities that could be used to select the influential InfoSec champions. In line with this theory, I analysed and found employees' provisions of instrumental resources, expressive resources and InfoSec support increase the likelihood of exerting InfoSec influence. This relationship between employees' socialisation and InfoSec influence was based on the theory's premises that when employees provide these resources, they exert influence over other employees by demonstrating their informational, expert and referent powers (Raven 2008).

Raven (2008) posits that the powers to reward and punish can enable individuals to exert influence over other people. These powers are relevant in the InfoSec context as employees' compliance with InfoSec policies has been found to be motivated by rewards (Bulgurcu, Cavusoglu & Benbasat 2010a; Pahnila, Siponen & Mahmood 2007; Siponen, Mahmood & Pahnila 2014) and sanctions (D'Arcy & Herath 2011; Herath & Rao 2009a, 2009b). Thus, these powers' impacts on the InfoSec influence over employees' InfoSec behaviours are worth examining. However, the testing of these powers' impacts on exerting InfoSec influence was not possible in this project, as TTT did not have any formal policies that informed employees about rewards and sanctions.

Reviews of behavioural InfoSec literatures (Lebek et al. 2014; Padayachee 2012; Sommestad et al. 2014; Warkentin & Mutchler 2014) did not report any prior studies that examined the theory of social power bases, especially for selecting InfoSec champions. As such, the ERGM analysis in this stage produced new knowledge concerning the behaviours of InfoSec influencers in the work context.

6.5.2 Reflection on the Selection of InfoSec Champions

I followed the recommendation of the action planning stage's instrumental theory, opinion leadership theory (Liu et al. 2017; Valente & Davis 1999), to select champions based on their out-degree centrality. The theory also suggested to use betweenness centrality and closeness

centrality when selecting influential leaders (Liu et al. 2017), but I decided not to use these measures in this stage because of their caveats (see Section 6.3.4). To compensate the limitation of out-degree centrality which focuses only on direct provisions of resources and direct InfoSec influence, I calculated employees' Beta centrality to capture their indirect influence in the networks (Borgatti, Everett & Johnson 2013).

I found the decision to use which centrality measures for identifying opinion leaders to be dependent on the practical context of the change program. Given the unique context of this project, which concerned the diffusion of InfoSec support and InfoSec influence, I considered opinion leadership theory as partially applicable for the selection of champions. Practitioners and researchers who follow the approach that leverages opinion leaders should critically select the suitable centrality measures that can appropriately capture leaders' influence. While it was outside of this project's scope to employ statistical tests to determine the suitable centrality measures for capturing employees' InfoSec influence, I believed that pursuing this research direction would produce useful insights.

The ERGM results indicated that employees' background characteristics and socialisation increased the likelihood of exerting InfoSec influence. This suggested that practitioners and researchers should consider other traits and abilities, in addition to their network centrality, when selecting the champions. Prior studies that focused on the selection of InfoSec champions were scarce. Of these studies, Chipperfield and Furnell (2010) suggested appointing InfoSec champions who are in senior positions, trustworthy and able to deliver InfoSec messages tailored to specific audiences in the workplace. My findings about the positive impacts of employees' seniority, having the same department memberships and provisions of expressive resources such as trust were in line with Chipperfield and Furnell's (2010) recommendations. Moreover, Gabriel and Furnell (2011) discussed the potential use of personality tests to select champions. It would have been interesting to select the champions at TTT based on their personality traits per Gabriel and Furnell's (2011) discussion, but this approach would place extra burden on employees to complete a personality test in addition to the main survey.

The ERGM results in this stage extended current knowledge about the selection of InfoSec champions by revealing the structural mechanisms that facilitated InfoSec influence. While these structural mechanisms increased the likelihood for employees to exert InfoSec influence, the inclusion of their effects in the exponential random graph models negated other effects of employees' background characteristics on their influential status. This implied that the

importance of employees' traits for selecting InfoSec champions depended on the unique network structures of the work environments.

Overall, the stage's findings suggested that the selection of InfoSec champions should be based on a combination of multiple factors—employees' background characteristics and behaviours, employees' network centrality and the structural features of the networks that represented the focal work environments.

6.5.3 Reflection on Further Actions

Having reached a consensus with the top management on the selected InfoSec champions, the project team could move to the next action taking stage. The original objective to follow the train the trainers approach and have the champions diffuse InfoSec knowledge, as stated in the diagnosis stage (see Chapter 5), remained unchanged.

A major research activity in this action planning stage was to analyse the networks representing the provisions of organisational resources and the InfoSec influence network to understand more about the current work environment at TTT. Further, these networks and their descriptive statistics served as the baseline findings that would be used to evaluate the effectiveness of the InfoSec champions' activities and the InfoSec change program in a later evaluation and reflection stage. Given the command-and-control model currently visible in the InfoSec-related networks, an objective of the InfoSec change program was determined to increase the density of these InfoSec-related networks. The change program should also reduce these networks' centralisation by having the appointed InfoSec champions diffuse InfoSec knowledge and emerge as the new sources of InfoSec support and influence.

At the beginning of this stage, the potential for employees to refuse to answer the sensitive questionnaire which asked employees about whom they socialised with in the workplace was a concern. However, the email from the General Director, which was sent to all employees and clearly stated that top management would not have access to the collected responses, appeared to be effective. The responses came quickly and throughout the data collection process the project team did not receive any complaints from employees.

The top management at TTT and the Vice Director of the BSP department displayed great interests and excitement when they analysed the network visualisations of employees' socialisation. The employees in TTT at this point had familiarised themselves with the

procedure of responding to the questionnaire, a sensitive matter and prone to non-responses (Borgatti, Everett & Johnson 2013). On this basis, the project team had acquired the buy-ins from top management and employees which were critical for the CAR project. I felt confident that employees would continue to support the project in the subsequent action taking stage where I would launch the questionnaire again to capture the changes in the InfoSec-related networks and InfoSec climate.

6.6 Chapter Summary

This chapter described and discussed the research activities in the CAR project's action planning stage. These involved conducting SNA to examine the networks within TTT and using the analysis outcome to select InfoSec champions for the InfoSec change program (i.e., diffusion of InfoSec knowledge). The InfoSec-related networks examined in this stage will later be used as a baseline for comparing with the post–InfoSec change program networks and to evaluate any changes.

I adopted the theory of social power bases (French & Raven 1959; Raven 2008), graph theory (Barnes & Harary 1983) and opinion leadership theory (Liu et al. 2017; Valente & Davis 1999) to determine the characteristics and interactions that made an employee capable of influencing others' InfoSec behaviours. The Vice Director of the BSP department and I jointly designed a questionnaire to collect the network data, and the ERGM method was employed to statistically validate the theoretical propositions of those theories.

Overall, the InfoSec-related networks before the change program were sparse (i.e., had low density and had high centralisation) and most of employees received InfoSec support and influence from a handful of IT and BSP staff. The top management and Vice Director of the BSP department commented that such networks reflected a current command-and-control InfoSec management model at TTT which had existed without their knowledge. At the end of the action planning stage, the project team and top management reached a consensus on the list of identified InfoSec champions for the change program. A summary of this stage's activities is presented in Figure 6.12.

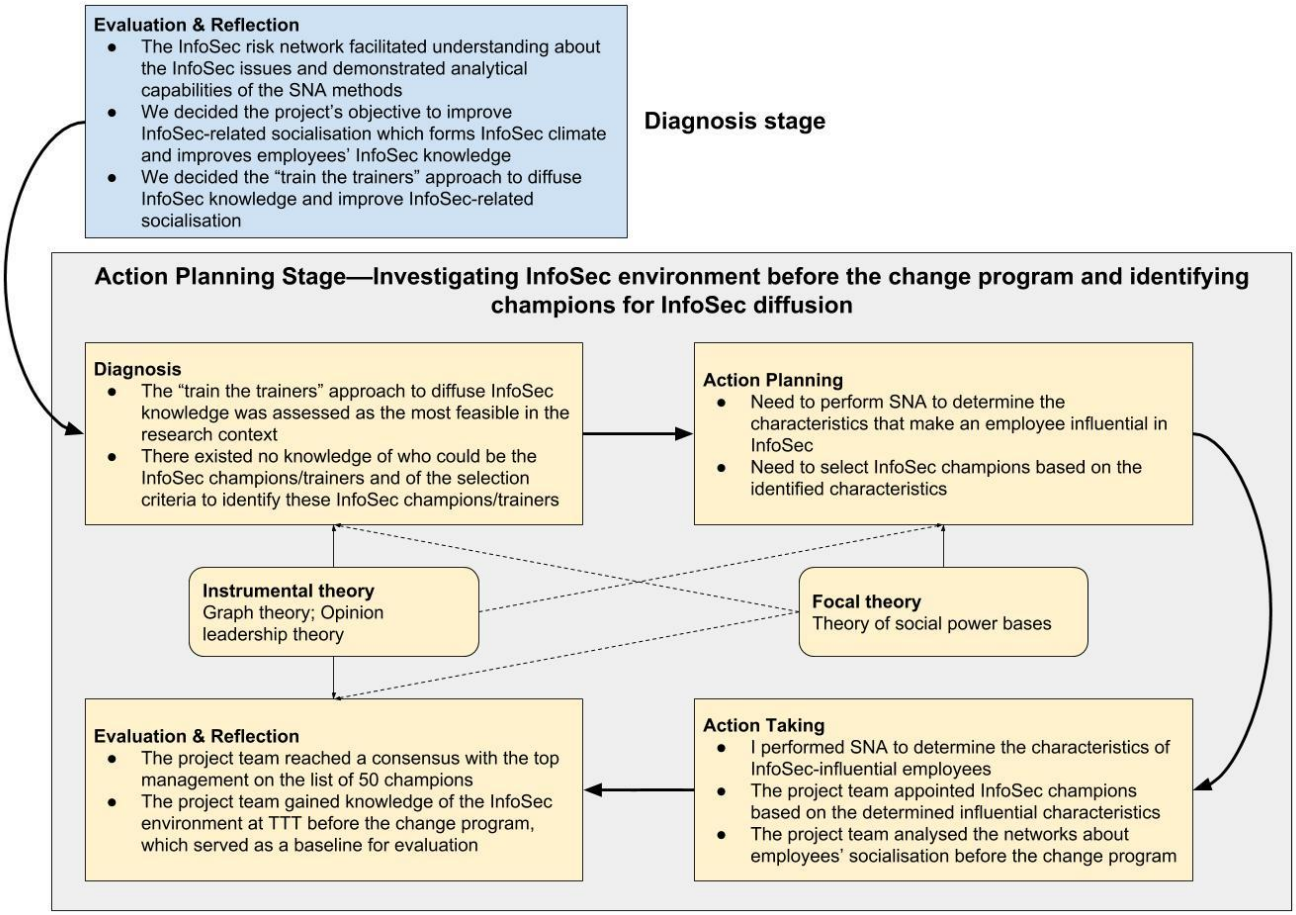


Figure 6.12. Summary of the Action Planning Stage

Chapter 7: Action Taking Stage—Conducting InfoSec Training for the Champions and Implementing the InfoSec Change Program

This chapter discusses the action taking stage of the CAR project, the diffusion of InfoSec knowledge. This stage aimed at preparing the 50 selected champions for the diffusion, through a change program following the train the trainers approach, to improve TTT's InfoSec environment. In this action taking stage, the diagnosis section focused on understanding the current situation—the champions had never received formal InfoSec training before and needed to be prepared for the diffusion of InfoSec knowledge. The action planning section reviewed the relevant literatures to learn about the key elements and approaches for effective InfoSec training, and the action taking stage involved carrying out the training. The training outcomes were then discussed in the evaluation and reflection sections. The structure of this chapter is presented in Figure 7.1.

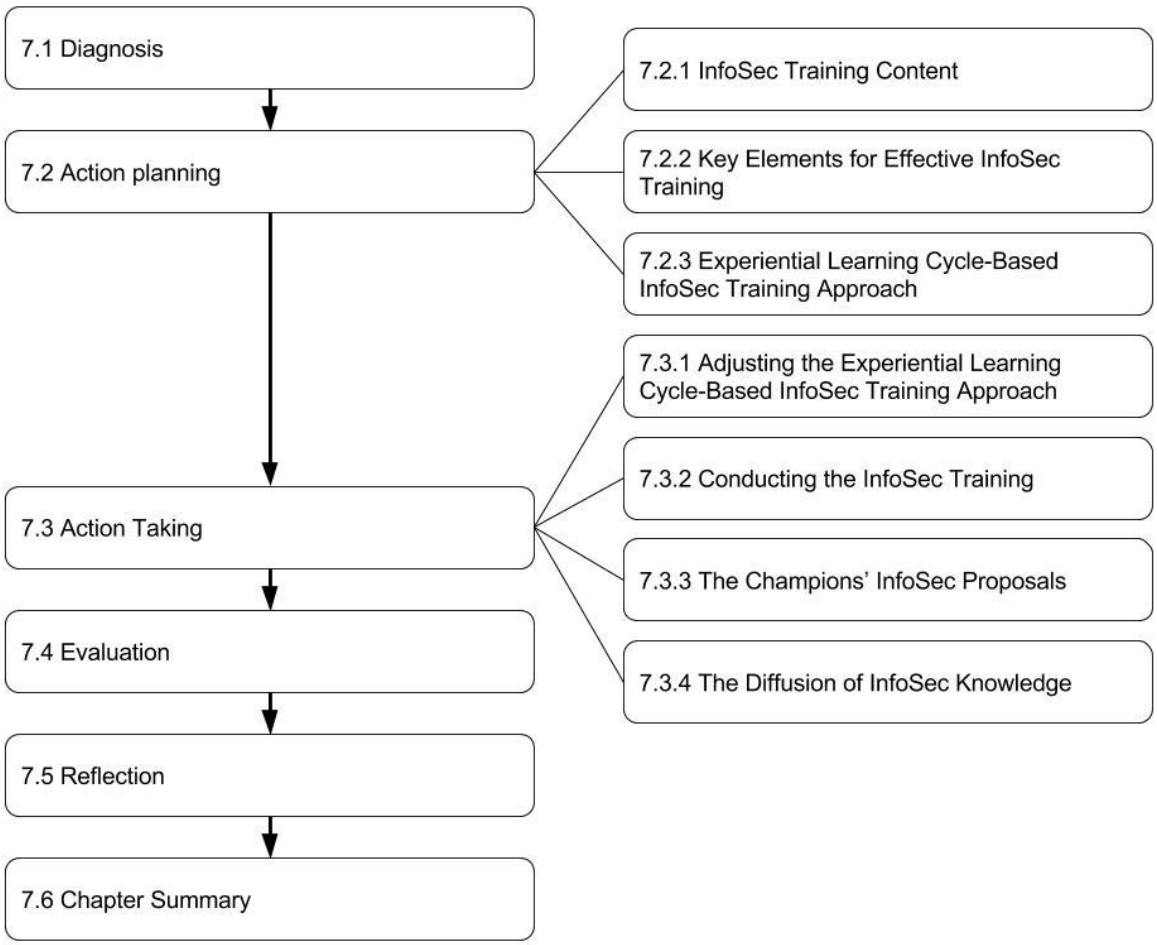


Figure 7.1. Structure of Chapter 7

7.1 Diagnosis

In the action planning stage of the CAR project I examined the InfoSec environment of TTT before the change program, which aimed at improving InfoSec climate and employees' InfoSec-related socialisation (i.e., their exchanges of InfoSec support and InfoSec influence). To that end, top management and I reached a consensus on the identification of 50 influential InfoSec champions to diffuse InfoSec knowledge, following the train the trainers approach as suggested by the interviewed InfoSec experts in the diagnosis stage (see Chapter 5).

The sparse networks of the InfoSec-related socialisation, dominated by a handful of IT and BSP employees, reinforced the adoption of the train the trainers approach that made use of InfoSec champions who would spread InfoSec knowledge. However, the selected InfoSec champions had never received any formal InfoSec training at TTT, and thus had varied to no InfoSec knowledge. Therefore, the project team decided to design and deliver InfoSec training to these champions before they started the diffusion of InfoSec knowledge.

7.2 Action Planning

As this stage focused on designing the appropriate InfoSec training materials and delivering training workshops to the selected InfoSec champions, the project team which would perform the training had to decide on the training content and how the training should be conducted. Once the training content and the delivery method were finalised, the project team would conduct training for the champions.

7.2.1 InfoSec Training Content

Organisational InfoSec programs often aim at improving employees' awareness of existing threats and vulnerabilities within the workplace and increasing their knowledge and confidence when handling InfoSec incidents (D'Arcy, Hovav & Galletta 2009; Furnell & Thomson 2009; Shaw et al. 2009; Workman, Bommer & Straub 2008). Straub and Welke (1998) stated that InfoSec training should educate employees on information about security risks and countermeasures. Topics concerning compliance and noncompliance should also be covered in InfoSec training. For example, communication about the certainty and severity of sanctions were emphasised as a method to deter potential InfoSec violations (Straub & Welke 1998).

Later studies suggested that InfoSec training programs should address topics such as InfoSec policy, procedures and responsibility (Bartnes, Moe & Heegaard 2016; Karjalainen et al. 2013; Straub & Welke 1998; da Veiga & Martins 2015). An emphasis on accountability and responsibility during training has been put forward by recent studies which found that employees tend to justify their noncompliance by using neutralisation techniques such as 'denial of responsibility', 'appeal to higher loyalties' (i.e., justifying a violation of InfoSec policy as a necessary requirement for achieving an important task) or 'metaphor of the ledger' (i.e., using previous good acts as an excuse to justify occasional violations of InfoSec policy) (Barlow et al. 2013; Siponen & Vance 2010). Further, research has reinforced that employees need to realise the consequences of InfoSec violations (Karjalainen & Siponen 2011; Puhakainen & Siponen 2010). Training modules that focus on employees' moral and ethics were also recommended (D'Arcy & Devaraj 2012; Hovav & D'Arcy 2012).

InfoSec training should help employees recognise the protective measures in the workplace, availability and effectiveness (Herath & Rao 2009a). InfoSec training should also boost employees' confidence in using InfoSec measures when necessary in real situations (Albrechtsen 2007; Cone et al. 2007; Siponen, Mahmood & Pahnila 2014). Being proficient in handling InfoSec incidents requires not only improving one's own knowledge, but also effective interactions with others. Therefore, cooperation and collaboration with peers and the ability to realise top management's InfoSec vision are some of the key abilities that need to be trained (Bartnes, Moe & Heegaard 2016; Thomson, von Solms & Louw 2006; da Veiga & Martins 2015). These skills cover how to report InfoSec incidents and, for the InfoSec champions, the diffusion of the learned knowledge to other colleagues; the latter is termed 'cascading training' or train the trainers approach (Bartnes, Moe & Heegaard 2016; Heikka 2008; da Veiga & Martins 2015).

The training contents suggested by the reviewed literature were consistent with the interviewed InfoSec experts' recommendations. In addition to the primary objective of improving employees' InfoSec awareness and knowledge through training, the InfoSec experts suggested that employees need to be informed about the outcomes of their compliance such as the protection of organisational InfoSec, the avoidance of sanctions and recognition and the outcomes of noncompliance such as sanctions and loss of productivity and time. The experts emphasised that InfoSec accountability and responsibility should be expected in the workplace by default, but some employees may fail to realise that and have to be reminded. Although the

experts recommended educating employees on the available InfoSec measures in their interviews, they did not put emphasis on communicating the measures' effectiveness. As the literature argued for the importance of raising employees' awareness of the measures' effectiveness (Herath & Rao 2009a; Vance, Siponen & Pahnila 2012), the project team decided to incorporate this content and the other topics discussed above into the InfoSec training.

While there are no one size fits all curricula for InfoSec training programs due to every organisation's unique needs (D'Arcy & Hovav 2008; Karjalainen et al. 2013), advice about the design of InfoSec training's topics can be found in industry guidelines. NIST (Wilson & Hash 2003) distinguishes InfoSec awareness and training programs, with the former focusing on providing information about InfoSec to employees while the latter aims at teaching InfoSec skills. In TTT's context, top management and the project team decided to pursue both objectives, raising employees' understanding about the importance of InfoSec and educating them on the basic InfoSec practices such as locking computer screens, checking for anti-virus software's updates and detecting and reporting InfoSec vulnerabilities.

The NIST guide provides a list of 27 key InfoSec topics such as passwords usage, web usage, spam, visitor control and email etiquette, and explains that the selection of InfoSec topics for the awareness and training programs should be based on the organisation's needs assessment (Wilson & Hash 2003). To this end, the project team had conducted the risk assessment in the diagnosis stage to identify the InfoSec issues and understand the current InfoSec environment at TTT. Based on the suggestions from prior studies, the interviewed experts and the NIST guide, the project team jointly selected the topics of the InfoSec training program at TTT which were then reviewed and approved by top management. Top management and the project team decided that the InfoSec training program should cover the following seven topics:

1) fundamental InfoSec concepts (i.e., confidentiality, integrity and availability and the roles of employees in protecting organisational InfoSec)
2) InfoSec threats (i.e., types of internal and external InfoSec threats)
3) malware (i.e., types of malware and their infection mechanisms)
4) internet usage (i.e., how to detect suspicious websites and tools for assessing websites' safety)
5) email usage (i.e., how to detect and report suspicious emails)
6) computers and data protection (i.e., management of physical and electronic files and how to backup data)
7) passwords usage (i.e., how to setup strong passwords).

7.2.2 Key Elements for Effective InfoSec Training

The relevant literature was reviewed to identify the elements of effective training. The four key elements for effective InfoSec training were identified to be 1) collaborative learning, 2) critical reflection, 3) relevancy and 4) facilitating conditions. These elements are summarised in Table 7.1 and below.

Table 7.1. Key Elements of InfoSec Training

Key element	Description	References
Collaborative learning	Training should be conducted in groups which facilitates sharing of ideas and construct collective knowledge among learners as well as with instructors	Albrechtsen (2007); Albrechtsen and Hovden (2010); Bartnes, Moe and Heegaard (2016); Heikka (2008); Karjalainen et al. (2013); Karjalainen and Siponen (2011); Puhakainen and Siponen (2010); Siponen, Mahmood and Pahnila (2014)
Critical reflection	Learners are encouraged to critically reflect on their learning which enables them to internalise and apply the learned knowledge	Albrechtsen and Hovden (2010); Cone et al. (2007); Heikka (2008); Karjalainen et al. (2013); Karjalainen and Siponen (2011); Puhakainen and Siponen (2010); Shaw et al. (2009); Thomson, von Solms and Technikon (2006)
Relevancy	Training materials and methods should be personalised and relevant to individual learners or groups	Albrechtsen (2007); Albrechtsen and Hovden (2010); Barlow et al. (2013); Bartnes, Moe and Heegaard (2016); Caldwell (2016); Chipperfield and Furnell (2010); Cone et al. (2007); D'Arcy and Hovav (2008); Furnell and Thomson (2009); Heikka (2008); Hovav and D'Arcy (2012); Karjalainen et al. (2013); Karjalainen and Siponen (2011); McCormac et al. (2016); Parsons et al. (2010); Puhakainen and Siponen (2010); Shaw et al. (2009); Siponen, Mahmood and Pahnila (2014); Siponen and Vance (2010); Straub and Welke (1998); da Veiga and Martins (2015); Zafar (2013)
Facilitating conditions	The arrangement of a training workshop should take into consideration the workshop's atmosphere, the instructor's creditability and organisational and national cultures	Albrechtsen and Hovden (2010); Caldwell (2016); Cone et al. (2007); Herath and Rao (2009a); Hovav and D'Arcy (2012); Karjalainen et al. (2013); Karjalainen and Siponen (2011); Parsons et al. (2010); Puhakainen and Siponen (2010); Straub and Welke (1998); Thomson and von Solms (1998); Zafar (2013)

The collaborative learning approach aims at promoting active exchanges between learners and instructors during the training process, which allows all training participants to co-discover and co-construct knowledge together (Gallivan et al. 2005; Karjalainen et al. 2013; Karjalainen & Siponen 2011). This training approach allows the learners to relate to their own InfoSec-related experiences and develop shared organisational InfoSec practices, and satisfies the learners'

need to voice opinions and creates an enjoyable learning atmosphere (Albrechtsen & Hovden 2010; Karjalainen & Siponen 2011).

The collaborative learning approach follows the principles of social constructivist and constructivist learning theories (Karjalainen et al. 2013; Karjalainen & Siponen 2011; Puhakainen & Siponen 2010). Constructivist learning theory argues that knowledge is subjectively formed by groups of people within a socio-cultural setting (Adams 2006; Richardson 2003). Social constructivism as a version of constructivist learning theory highlights the social process, such as interactions and dialogues, which contributes to the construction of knowledge (Adams 2006; Richardson 2003). In constructivism-based pedagogical approaches, learners construct their own knowledge through their active participation in a process to make sense of their unique experiences which involve activities such as reflection, open-ended investigations and exchanges of ideas within a learning community (Adams 2006; Boghossian 2006; Fosnot & Perry 2005). As a result, constructivism puts emphasis on the learners, rather than the teacher, as the centre of knowledge (Boghossian 2006).

Unlike constructivist theories, behaviourism as a learning theory focuses on the teacher-directed, instructional and controlled transmission of objective knowledge and emphasises the frequent use of tests to ensure learners' mastery (Murphy 1997; Shepard 2000). Representatives of the behaviourist learning theory include instructor-led or computer-based InfoSec training and InfoSec campaigns which offer advantages for organisation-wide and standardised training solutions (Cone et al. 2007). Given that there were 50 InfoSec champions who needed to be trained intensively, the project team deemed the constructivism-based collaborative learning approach as suitable and appropriate for such a number of learners.

The learners' critical reflection on the learning materials is also a key element for effective InfoSec training. Reflection allows the learners to critically analyse the taught InfoSec practices, while incorporating their personal experiences which increases their confidence in applying the techniques when necessary. Reflection on the learned knowledge also creates long-lasting changes (Puhakainen & Siponen 2010). Having learners reflect on their personal InfoSec experiences can support their adoption of the InfoSec practices more easily, and the reflected experiences can contribute to the group discussion and further facilitate collective learning (Albrechtsen & Hovden 2010).

Relating to familiar and real-world issues enables learners to make personal connections with the taught knowledge, supports the development of ownership and mutual understanding about how InfoSec should be practiced (Albrechtsen & Hovden 2010; Chipperfield & Furnell 2010; Furnell & Thomson 2009; Karjalainen et al. 2013; Parsons et al. 2010; Puhakainen & Siponen 2010). While critical reflection and collaborative learning bring relevant experiences to the group discussion, facilitators should tailor the training to match different learning groups. Factors such as learners' proficiency in using computer and whether they are physically bound to the work environment should be taken into consideration (D'Arcy & Hovav 2008). This calls for a bespoke approach to design InfoSec materials that fit employees' interests, needs, roles or job functions (Chipperfield & Furnell 2010; Parsons et al. 2010). Since the project team had conducted the risk assessment in the diagnosis stage, the identified InfoSec threats and vulnerabilities in TTT were incorporated into the training.

Finally, the facilitating conditions are critical for successful InfoSec training. Budget constraints and appropriate training modes (e.g., presentation slides, lunch meetings and games) are both important when designing InfoSec training (Albrechtsen & Hovden 2010; Parsons et al. 2010). Training facilitators should engage with learners by using real InfoSec scenarios and framing suitable messages for different organisational audiences (Chipperfield & Furnell 2010; Cone et al. 2007). The facilitators' credibility also impacts learners' attitude towards learning (Puhakainen & Siponen 2010). Moreover, national and organisational cultures should be considered since these cultural factors could affect learners' learning styles. For example, the Confucian-based cultures of many Asian countries hold that moral plays a significant role in deterring undesired behaviours and employees refrain from engaging in malicious InfoSec behaviours since they feel the informal pressure from their group norms rather than the formal policy (Hovav & D'Arcy 2012). The dominant effect of social norms on employees' InfoSec behaviours had been mentioned by the interviewed InfoSec experts in the diagnosis stage. Thus, InfoSec training in such a context should focus on the mechanisms for raising employees' moral consciousness (Hovav & D'Arcy 2012). Understanding the organisational culture can reveal additional factors that show how InfoSec training should be delivered. For example, there are workplaces where practicing InfoSec can boost one's self-esteem and social status (Chipperfield & Furnell 2010). Depending on the local context, the training atmosphere can be informal, relaxing and even humorous, where the facilitators mainly stay in the background and avoid projecting an authoritative image (Albrechtsen & Hovden 2010).

The four key elements of collaborative learning, critical reflection, relevancy of training contents and facilitating conditions established the theoretical background of the InfoSec training at TTT and served as the focal theory for this stage, informing the subsequent design of the workshop and training materials. Some of these elements are grounded on educational theories, such as the collaborative learning and reflection on communally relevant experiences that follow the principles of constructivist learning theory (Miller 2007). The element of facilitating conditions is suggested by empirical studies rather than based on theories.

7.2.3 Experiential Learning Cycle-Based InfoSec Training Approach

The project team proceeded with selecting a suitable training method that satisfied the four key elements. Such a training method would serve as the instrumental theory for this stage of the CAR project. My review of the literature on InfoSec training did not find many studies that provided a detailed and step-by-step instruction to InfoSec training. Karjalainen and Siponen (2011) had also conducted a detailed review of 32 InfoSec training approaches and compared these against four pedagogical requirements for successful training: 1) explicit psychological context, 2) content, 3) teaching method and 4) evaluation for learning. These four requirements are explained below.

Learning theories, such as behaviourism and constructivism, establish the psychological context for InfoSec training (Karjalainen & Siponen 2011). Karjalainen and Siponen (2011) argued that InfoSec training should embrace a group-oriented approach as InfoSec training aims at creating communal changes (i.e., the group's collective ability to perform InfoSec behaviours in the complex workplace) rather than individual changes, hence advocating the adoption of constructivist pedagogy. On this basis, they discussed that the training content should reflect learners' collective experiences to effectively educate about InfoSec policies which will be collectively understood and accepted by the groups. The teaching method in this case would also follow collectivist principles, which emphasise collaborative learning and aim at delivering communal changes, and so would the evaluation method (Karjalainen & Siponen 2011). Specifically, Karjalainen and Siponen (2011) discussed that evaluation after InfoSec training should include learners' self-evaluation, reflection and continuous dialogues with the InfoSec trainer, rather than employing tests that concentrate on problem-solving ability and predefined responses.

IS security training approaches	(1) Fulfills the requirement for the explicit psychological context	(2) Fulfills the requirement for the content	(3) Fulfills the requirement for teaching method	(4) Fulfills the requirement for evaluation of learning
Cognitive processing approach (Puhakainen, 2006)	-	X	X	X
Social psychological recommendations approach (Kabay, 2002)	-	X	X	-
Andragogical approach (Herold, 2005)	-	-	-	X
Strategic approach (Wilson and Hash, 2003)	-	-	-	X
Pedagogical requirements: (1) the explicit psychological context must be based upon the group-oriented theoretical approach of teaching and learning; **(2) the training content** must be based on collective experiences of the learners; **(3) teaching methods** must focus on collaborative learning in order to reveal and produce collective knowledge; and **(4) evaluation of learning** should emphasize experiential and communication-based methods from the viewpoint of the learning community.				
Analyzed IS security training approaches, which do not fulfill any of the pedagogical requirements: Constructive instruction approach (Heikka, 2008); Constructive scenario approach (Biros, 2004); Cyber security game approach (Cone et al., 2007); Pedagogical game approach (Greitzer et al., 2007); Social psychology–oriented approach (Thomson & von Solms, 1998); Motivation theory directive approach (Roper et al., 2006); Persuasive technology approach (Forget et al., 2007); Normative approach (Siponen, 2000); Counteractive approach (McIlwraith, 2006); Security ensuring approach (Peltier, 2000); Communication-oriented approach (Desman, 2002); Promotional approach (Rudolph et al., 2002); Stakeholder approach, (Kovacich & Halibozek, 2003); Deterrence approach, (Straub & Welke, 1998); Academic environment approach (Kajava & Siponen, 1997); University environment approach (McCoy & Thurmond Fowler, 2004); Preventive approach (Nosworthy, 2000); Competence approach (Wilson et al., 1998); Operational controls approach (NIST, 1995); ISD approach (Hansche, 2001); Traditional e-learning approach (Kajava et al., 2003); Hypermedia instruction approach (Shawn et al., 2009); Policy creation approach (Gaunt, 1998); Healthcare environment approach (Furnell et al., 1997); Discursive approach and online tutorial approach (Cox et al., 2001); Briefing approach (Markey, 1989); Social engineering preventive approach (Mitnick & Simon, 2002) and; Active e-learning approach (Furnell et al., 2002).				

Figure 7.2. Evaluation of InfoSec Training Approaches

Adopted from Karjalainen and Siponen (2011, p. 535).

As none of the reviewed InfoSec training approaches fully met the four described requirements (see Figure 7.2), Karjalainen and Siponen (2011) proposed an InfoSec training program which follows the experiential learning approach (Gibson 2001; Kolb 1984). The experiential learning approach follows the principles of constructivist learning theory (Kolb & Kolb 2011; Yilmaz 2008). This approach focuses on a process of learning derived from and continuously modified by learners' experiences, rather than the outcomes of learning (Kolb & Kolb 2011; Kolb 1984). During that process, learners develop refined knowledge by integrating their unique beliefs and ideas with those of other learners through reflection and resolution of conflicts (Kolb & Kolb 2011).

Educators and trainers who adopt the experiential learning approach utilise a four-phase process model called 'experiential learning cycle'. The experiential learning cycle utilises four principal learning stages—concrete experience, reflective observation, abstract conceptualisation and active experimentation—which aim at enabling learners' experiencing, reflecting, thinking and acting respectively (Kolb & Kolb 2011). The experiential learning cycle commences with the learners who have unique experiences (the concrete experience stage), and they are then asked to reflect on these experiences by observing different perspectives (the reflective observation stage) (Akella 2010; Kolb & Kolb 2011). In the next stage, abstract conceptualisation, learners assimilate their reflection into abstract concepts and draw implications for actions which are taken in the subsequent stage, active experimentation (Akella 2010; Kolb & Kolb 2011).

The InfoSec training approach proposed by Karjalainen and Siponen (2011) consists of learning activities that guide learners through the four phases of experiential learning cycle described above. For example, Karjalainen and Siponen (2011) suggested focusing on understanding employees' own experiences about InfoSec threats, organisational assets and protection mechanisms in the first phase of the experiential learning cycle. These experiences hold critical roles since they not only facilitate the activities of the next learning stage, but also highlight the importance of InfoSec (Karjalainen & Siponen 2011). During the second phase, reflective observation, trainers can organise group-based learning activities such as the 'Think-Pair-Share' technique (Barkley, Cross & Major 2005). This training technique in the InfoSec context involves having employees work in pairs to develop a joint response about an InfoSec protection practice, then sharing responses with other pairs and the rest of the class (Karjalainen & Siponen 2011). Employees develop abstract concepts about InfoSec in the third phase by analysing the similarities and differences between their shared reflection and the organisation's InfoSec policy (Karjalainen & Siponen 2011). The abstract concepts are then discussed between the trainers and employees to formulate executable actions (e.g., a new InfoSec policy or InfoSec practice) and employees are asked to observe and reflect on their performed actions in the fourth phase. Such observation and reflection can be discussed in the next experiential learning cycle (Karjalainen & Siponen 2011).

Overall, my literature review provided the project team with information about the key elements of effective InfoSec training (see Table 7.1) and a detailed and theoretically-based training approach that could satisfy these key elements (Karjalainen & Siponen 2011).

However, the project team decided not to apply the same training procedure recommended by Karjalainen and Siponen (2011) without adjusting it to suit the unique context of TTT and the nature of this research project. Therefore, the project team, top management and the champions planned to perform four activities in total.

First, the project team and top management would discuss the necessary adjustments to the chosen experiential learning cycle-based InfoSec training approach to fit with TTT's unique work context. Second, the project team would conduct the training program with the champions, comprising four workshops and a task requiring champions to prepare InfoSec proposals. Third, the project team and top management discussed the InfoSec proposals and the diffusion approaches with the InfoSec champions. Fourth, the champions performed the diffusion of InfoSec knowledge as intended in this stage of the CAR project.

7.3 Action Taking

7.3.1 Adjusting the Experiential Learning Cycle-Based InfoSec Training Approach

The project team and top management discussed the four phases of the experiential learning cycle-based InfoSec training program as described above, which resulted in several adjustments to the training procedure. The project team and top management recognised that the champions or learners had not received any formal InfoSec training before, thus, their levels of InfoSec-related experiences were expected to be low and varied. Since the experiential learning approach relies on learners' unique experiences, the champions' low and inconsistent levels of InfoSec-related experiences could impact the training effectiveness. The project team then decided to establish a common context for the training by commencing the workshops with an introduction of the seven InfoSec topics as the learning objectives (see Section 7.2.1). As such, the champions would be encouraged to reflect on any of their previous InfoSec-related experiences relevant to the seven topics. For example, their experiences may include situations when they found a suspicious website or email, InfoSec threats such as unattended documents or a visitor who walked freely and unescorted in the office. The project team, as trainers of the workshops, would stimulate discussion by emphasising that any past InfoSec-related experiences, regardless of how trivial they might be, would be valuable for the learning process.

In the second experiential learning phase, Karjalainen and Siponen (2011) suggested that learners share ideas in pairs, the pairs share ideas in groups of four and, finally, present their

ideas to all learners attending the workshop. However, top management would only allow each workshop to be run for two hours due to the champions' tight work schedules. If the project team followed Karjalainen and Siponen's (2011) suggested learning activity, then its procedure would need to be replicated seven times for each of the seven InfoSec topics. Such activity would not be completed within the allowed two hours, and the project team was also concerned that the champions would be exhausted by the repeated procedures. The project team decided that, after the brief introduction of the seven InfoSec topics, the champions would discuss their past InfoSec-related experiences and ideas in the format similar to a focus group. It was important that all champions who attended the workshop would be encouraged to contribute their experiences and ideas, while the trainers would facilitate the discussion in the background.

In the third phase, the suggested learning activity involved the trainers introducing the organisation's InfoSec policies to the learners, then allowing the learners to analyse the similarities and differences between their discussed ideas and the InfoSec policy (Karjalainen & Siponen 2011). Since TTT did not have any formal InfoSec policy, the project team prepared the recommended InfoSec practices based on industry standards and guides (e.g., NIST and ISO 27001) and explained these practices to the champions. The lack of official InfoSec policy and InfoSec practices could also be used to stimulate the champions' contributions during the workshops, by emphasising that their participation would contribute to the development of TTT's future InfoSec policy and practices. After the best InfoSec practices were introduced, the champions compared their InfoSec-related experiences and ideas against the best practices and contributed insights to the discussions.

The fourth phase of an experiential learning cycle focuses on the learners implementing the agreed actions and their evaluation of performance through dialogues with the trainers and other learners in the next learning cycle (Karjalainen & Siponen 2011). To facilitate discussions about InfoSec actions, the project team decided to have the champions formulate InfoSec proposals which detail their proposed InfoSec solutions to the InfoSec issues in their departments. The due date for this activity was set one week after the workshops. The project team also mentioned at the end of the workshops that the champions' roles included diffusing InfoSec knowledge to their colleagues. Table 7.2 lists the four phases, their activities, the project team's assessment of their feasibility and the adjustments made to fit the context of TTT.

Table 7.2. The Modified Experiential Learning Cycle-Based InfoSec Training Approach to Fit the Local Context

Suggested learning activities	Feasibility in TTT's context and considerations	Adjustments to learning activities and estimated time
Phase 1 (Concrete experiences) Learners form the basis of learning by reflecting on their individual experiences about InfoSec assets, threats and protective means.	The champions had not received formal InfoSec training before and their InfoSec-related experiences might be inconsistent and at a low level. The project team also decided to educate the champions about seven InfoSec topics (see Section 7.2.1). Therefore, it would be necessary to establish a common context for the workshop.	The project team as trainers commenced the workshop by presenting about the key InfoSec concepts which were aligned with the seven InfoSec topics to be covered in the workshop. The champions were asked to reflect on and to discuss their past experiences about the presented concepts. A brief introduction of the seven InfoSec topics was conducted in less than 15 minutes on presentation slides.
Phase 2 (Reflective observation) Learners share ideas in pairs and pairs share ideas in groups of four, then the shared ideas are shared with all members attending the workshop.	Each workshop is limited to two hours, which is not suitable to conduct the suggested procedure for each of the seven InfoSec topics.	The champions attending the workshop discussed InfoSec-related experiences and ideas with each other and with trainers in the format similar to a focus group. This ensured the workshops to meet the time requirement. The sharing of InfoSec-related experiences and ideas should be conducted within one hour.
Phase 3 (Formation of abstract concepts and generalisations) Trainers explain InfoSec policy and InfoSec practices, then learners analyse the differences and similarities between their discussed ideas and the explained policy/practices.	TTT did not have any InfoSec policy and InfoSec practices. Moreover, the champions' lack of InfoSec-related experiences may discourage them to share ideas.	The project team introduced the best InfoSec practices that were based on industry standards and guides. The champions compared the similarities and differences between their InfoSec-related experiences and the best practices.
Phase 4 (Active experimentation) Trainers and learners discuss ideas and reach a consensus on the actions to be taken i.e., new InfoSec practices and/or	The suggested procedures were feasible in TTT's context.	After the workshop, the champions were asked to develop InfoSec proposals which detailed their proposed InfoSec solutions to mitigate

revised InfoSec policies. Learners are asked to observe and reflect on their performed actions. The performed actions can be evaluated through dialogues with the trainers and with other learners in the next experiential learning cycle.		the InfoSec issues in their departments. The project team discussed InfoSec proposals with the champions after the workshops to reach a consensus on the proposed InfoSec solutions.

7.3.2 Conducting the InfoSec Training

The project team took action and conducted four training workshops with 50 InfoSec champions in two days. Each workshop was attended by 11 to 15 champions. Champions who worked in the same department were encouraged not to participate in the same workshop to ensure diversified experiences for discussion. Table 7.3 presents the numbers and compositions of participants in each workshop.

Table 7.3. Training Workshops and Participants

Training workshop (# of participants)	Champion ID (1–50)	Department	Note
Training workshop 1 (13 participants)	1	Accounting	
	19	Construction	
	20	Construction	
	21	Construction	
	33	Gamma	
	36	Human resource	
	37	Human resource	
	38	Marketing	
	40	Project management	
	45	Purchasing	
	46	Purchasing	
	48	Quality control and assurance	
	49	Tender	
Training workshop 2 (11 participants)	5	Architect	
	16	BSP	
	18	Business development	
	22	Construction	
	23	Construction	
	35	Hanoi	Online
	41	Project management	
	42	Project management	
	43	Project management	
	47	Purchasing	
	50	Tender	
Training workshop 3 (15 participants)	6	Architect	
	7	Architect	

	8	Architect	
	9	Architect	
	10	Architect	
	11	Architect	
	12	Architect	
	13	Architect	
	14	Architect	
	28	Factory	Online
	29	Factory	Online
	30	Factory	Online
	31	Factory	Online
	32	Factory	Online
	27	Factory	Online
Training workshop 4 (11 participants)	2	Accounting	
	3	Administration	
	4	Administration	
	15	After sale services	
	17	BSP	
	24	Construction	
	25	Estimation	
	26	Estimation	
	34	Gamma	Online
	39	Marketing	
	44	Project management	

The project team acted as facilitators and opened each workshop with a presentation covering the seven selected topics. We briefly explained to the champions the concepts and definitions of InfoSec, such as the importance of InfoSec in TTT's context, the possible routes of cyberattacks and online threats on the internet. Real examples of InfoSec incidents and threats, documented by the BSP and IT departments and from the risk assessment in the diagnosis stage (see Chapter 5), were also included in the presentation slides.

After the brief presentation about the InfoSec topics, the champions were asked to discuss their relevant InfoSec-related experiences. The common experiences discussed by the champions included the organisation and safeguard of hardcopies and computer files in the departments, internal and external files transfers and information leakage to clients or business partners. Based on the discussed InfoSec-related experiences, the project team then suggested the best InfoSec practices and let the champions analyse these practices.

For example, the Vice Director of the BSP department reminded the champions about the company's cloud which offered a secure mean to transfer files internally and externally. However, the champions mentioned that besides sending files as email attachments to external

recipients in daily work, they also shared files by using personal online storages such as Dropbox and Google Drive. Some champions reported that they even saw their colleagues send work files to others and external recipients by using the chat function of Facebook. They explained the reasons for not using the company's cloud were employees' lack of awareness about the cloud and the inconvenience caused by poor usability and slow speed. After discussing the pros and cons of using the company's cloud instead of personal clouds such as Dropbox and Google Drive, the project team convinced the champions to adopt the company's cloud for future transferring of files and diffuse such information to their colleagues. The Vice Director of the BSP department also committed to improve the company's cloud by addressing the feedback from the champions during the workshops. Overall, the atmosphere of the four workshops was kept relaxed and open for discussion, where the project team members stayed in the background as facilitators and let the champions actively engage in an exchange of information and opinions.

7.3.3 The Champions' InfoSec Proposals

At the end of the workshop, the InfoSec champions were given the task to prepare InfoSec proposals which suggested the InfoSec solutions that they believed could alleviate the InfoSec threats in their departments. A sample InfoSec proposal prepared by the champions in the construction department is presented in Figure 7.3.

By asking the champions to prepare the InfoSec proposals the project team achieved two things. First, completing the first part of the proposals about InfoSec issues required the champions to critically analyse the InfoSec environment in their departments. This provided them with an opportunity to reflect on and review their new knowledge. Second, the learned knowledge could be directly applied to generate a list of proposed solutions to mitigate the InfoSec issues identified by the champions themselves. Since these solutions were formulated by the champions, including the suggestion to provide InfoSec training to other employees, they were highly relevant to the champions' contexts and created a sense of ownership that would subsequently encourage the champions to enact the proposed solutions.

Information security issues

Issue	Description
1. Documents at the construction sites can be loss or stolen	- We only have temporary shelves to store documents at construction sites. There are no locks or only weak ones - Computers at the construction sites are shared; files and information about the projects can be lost or stolen easily
2. Information on computers can be read/eavesdropped	- Employees don't have the habit to log out when leaving their computers, which allows information on the computer's screen can be read
3. Lack of appropriate/planned files and folders management on the department's shared drive; the files and folders are also not secured	- Many people have access to the shared drive so information about worker's salary, allowance etc. is not secured and can be easily stolen - The department's shared drive has many unofficial and temporary folders since anyone can create folders for whatever purpose - No naming convention for files and folders - Anyone in the department can see and delete, or accidentally move the folders or files to another location - No specific access rights to the shared drive (e.g. secretaries should be able to see document files only; designers and architects should only have access to blueprints and databases etc.)
4. Loss of information on TEMP drive	- Employees have the habit to leave information about projects on the TEMP drive. As a result, the information can be lost or stolen.
5. Information can be copied illegally	- Company's data about construction projects can be copied for personal uses
6. Capture and post photos of manufacturing workshops and construction sites on Facebook and other online public sites	- Staff take photos of ongoing projects and post on Facebook

Information security solutions

Solution	Description
1. Construction sites need secure lockers. The information in important documents needs to be stored in computer systems	- Only one responsible employee of each construction team should keep the keys to all secure lockers that contain confidential documents - Important documents need to be scanned and saved in SharePoint; projects saved on SharePoint should be accessed by only designated employees
2. Software	- Purchase software which can automatically create folders based on pre-defined conventions - Limits copying files
3. Procedures and training	- Documentation of detailed instructions for old and new employees to perform work within their own responsibilities or work domains
4. Meetings to discuss and remind employees about information security issues	- Conduct meetings in small teams to discuss information security issues and remind people about following information security procedures
5. Clear job responsibilities and access rights to work files and folders	- Limit employees' access to files and folders that are unrelated to job responsibilities - Design clear job responsibilities and access rights to work files and folders
6. Folders management	- Each project needs to have a folder on TEMP drive and set access rights to specific employees; only employees in-charge of the project should have access to that project's files and information. - Staff can set passwords for their personal folders
7. Install CCTVs in areas with important documents	- Areas that are used to store confidential documents need to have CCTVs

Figure 7.3. InfoSec Proposal Prepared by Champions of the Construction Department

Although the due date for submitting the InfoSec proposals was set as one week after the workshops, it took a month for the champions of all departments to submit the InfoSec proposals. The project team reviewed the InfoSec proposals with the top management and had two one-hour meetings with the champions to discuss and clarify the proposals. The proposed InfoSec solutions included improvements in the areas of InfoSec infrastructure and employees' InfoSec knowledge.

The proposed infrastructure-related improvements included the allocation of more secure lockers, encrypted USBs and portable drives to the departments and installing CCTV at the

construction sites as seen in the sample proposal (see Figure 7.3). Champions also requested to adjust the levels of access rights to their departments' shared network drives. It appeared that many InfoSec champions were dissatisfied with the current setup that allowed access rights to shared folders across departments. Champions from the construction, HR, sourcing and planning departments also suggested more meeting rooms for confidential discussions. The champion from the HR department, who was also the department's director, complained that job interviews were sometimes inappropriately conducted at a meeting table in the public area. He argued that such discussions in the public area may expose confidential information about the candidates and salary. Similarly, the champions from the construction department also raised the issue of lacking private meeting rooms and storage for confidential documents at the construction sites. Moreover, they explained that the situation at the construction sites was risky as the discussions and documents were exposed to contracted workers and business partners such as subcontractors and clients.

There was a debate during a meeting to discuss the InfoSec proposals about whether personal devices and software applications such as laptops, portable drives and personal email accounts should be used for work purpose. The InfoSec champions of the architect department opposed this suggestion as they saw the use of personal devices and software applications as a threat to organisational InfoSec. These champions also proposed banning the use of online social media in the workplace and restricting access to several suspicious websites. The other champions argued that such restrictions would not be an ideal solution and proposed to focus on educating employees with proper InfoSec knowledge instead.

The project team took note of these concerns and consulted top management after these meetings. The agreed solution was a long-term strategic plan which aimed at revising the budgets to purchase more IT equipment such as laptops, USBs and portable drives for work purposes and secure lockers. In future, each department will be allocated secure USBs and portable drives kept by the department's champions. Personal laptops with InfoSec functions (e.g., anti-virus software, auto-backup software and remote wipe functions) will be provided to employees on demand.

It was also argued that the IT and BSP departments in the future would look for the technical solutions to monitor and manage employees' personal internet use more effectively, rather than banning all non-work activities. Further, the Vice Director of the BSP department initiated a

new project to resolve issues pertaining to access rights, especially the management of the publicly shared 'TEMP' file directory[4].

The champions provided suggestions for the diffusion of InfoSec knowledge in the meetings. For example, champions of the architect and construction departments suggested diffusing information about the procedures for managing and processing documents and computer files at various levels of seniority. Such information was essential for these departments and their employees since they handle large volumes of documents and files daily. The champions of the planning and estimation departments proposed to train their colleagues about secure email practices, such as carefully checking that the correct recipients were included in the email, removing unintended attachments before forwarding emails and developing a clear understanding about which information could be disclosed to whom internally and externally.

Information about dealing with visitors was mentioned in the InfoSec proposals of the factory and sourcing departments. Since the factory often invited clients and business partners to the manufacturing site to showcase the furniture's models, mock rooms and decorated spaces, they considered the external visitors as a potential InfoSec threat. Specifically, InfoSec champions of the factory departments felt concerned that these visitors might take photos of the machinery and design models, some of which were TTT's confidential assets. They proposed training their colleagues about visitor control practices, such as requesting external visitors to wait at a designated area in the office or to escort the visitors to the intended locations instead of letting them freely walk there unescorted. Additionally, the champions proposed to develop a work culture where employees would be constantly reminded that no visitors were permitted to take photos or record audio inside the factory.

The champions also reported incidents where employees had forgotten their printed documents at the shared printers or recycled papers that contained sensitive information. In this regard, champions of the tender and planning departments committed to training their colleagues in secure printing practices. The champions of the marketing department were rather creative as they suggested using the email calendars to remind staff about performing InfoSec practices,

[4] TTT created the 'TEMP' file directory as a way for sharing files internally; all employees had access to this directory, could upload files or create folders and recipients would download the shared files or folders from there. Issues related to the 'TEMP' file directory were discussed in Chapter 4 of this thesis.

such as checking for new anti-virus software updates or archiving confidential documents received during the day in the designated safe locations.

7.3.4 The Diffusion of InfoSec Knowledge

In the meetings before the diffusion, three champions expressed their concern that even though they were interested in InfoSec matters, they were not confident in their communication skills and ability to influence others' InfoSec behaviours. Some champions also reported that they had never prepared training slides before. In response to these issues, the project team and top management devised two diffusion methods. First, the champions experienced in delivering training volunteered to design the training slides that they believed would be appealing to the general audience in TTT. The champions from project management volunteered to design the training slides as they had organised large-scale training on enterprise resource planning and customer relationship management systemsfor other departments in the past. Second, top management agreed that only large departments of more than 10 employees would require the champions to conduct formal training sessions. Small departments of fewer than 10 employees could organise an informal discussion to review the training slides. The project team and top management also requested the champions to occasionally remind their colleagues about InfoSec matters during the diffusion period.

After the two meetings to discuss the InfoSec proposals, the InfoSec champions immediately commenced the diffusion of InfoSec knowledge in their own departments for four months. The period of four months was decided by the project team and agreed upon by top management for two reasons. First, it was decided to fit into the PhD candidature's allocated time frame of four years, with the diffusion of InfoSec knowledge taking place in the third year. By completing the diffusion and its evaluation before the end of the third year, I could use the fourth year of my PhD candidature to finalise the thesis. Second, expert opinions suggested that it would take a minimum of three months to evaluate an InfoSec implementation such as the ISO 27001 standard[5].

[5] For example, the British Assessment Bureau, a certification company acknowledged by ISO, suggested that an ISO 27001 certification normally takes 3 to 6 months (http://www.british-assessment.co.uk/guides/iso-27001-beginners-guide/ [accessed 18 September 2017]). Another ISO certification body, NQA, advised that an organisation should have their ISO 27001 implemented and fully operate for at least 3 months before an evaluation can be conducted (https://www.nqa.com/en-us/resources/blog/december-2015/your-complete-guide-to-the-iso-27001-standard [accessed 18 September 2017]).

The project team did not interfere in the champions' diffusion of InfoSec knowledge. This was to ensure that the outcome of the diffusion would accurately reflect the champions' influence on the InfoSec environment at TTT, rather than being pressured by the project team to achieve the desired improvements. The outcome of the champions' diffusion of InfoSec knowledge will be evaluated in the next stage of the CAR project. Figure 7.4 presents a summary of the research activities described so far—the adjusted four-phase experiential learning cycle-based InfoSec training, the preparation of and discussion on the InfoSec proposals and the champions' diffusion of InfoSec knowledge.

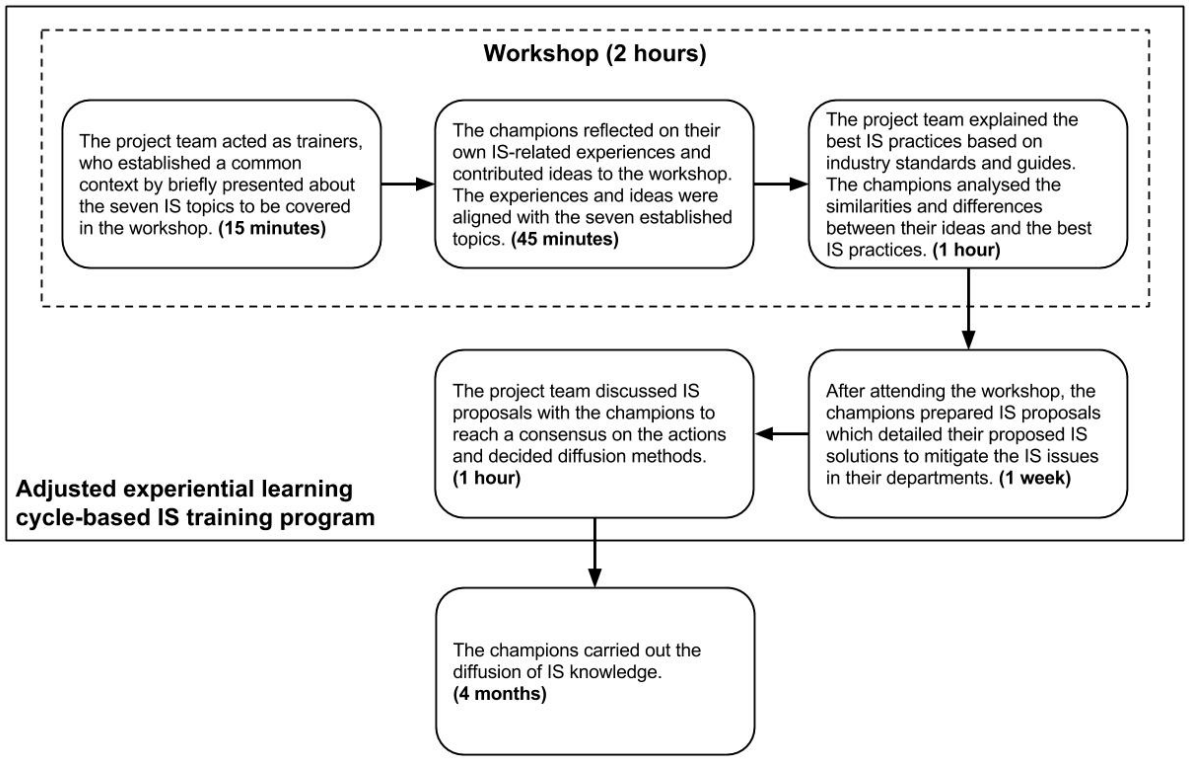


Figure 7.4. Summary of Research Activities

7.4 Evaluation

The workshops were conducted with full attendance of 50 champions appointed in the previous action planning stage. Informal discussions between the project team and the InfoSec champions after the workshops indicated that the champions enjoyed the workshops. The InfoSec champions were glad to see TTT's serious commitment to InfoSec matters in the workplace and confirmed that the workshops had enhanced their understanding about InfoSec.

At the end of the training program the project team and top management collected InfoSec proposals from the champions, which allowed the champions to voice their opinions about their

desired InfoSec improvements in their work settings. The champions' suggestions led to the initiations of formal projects which aimed at improving the InfoSec environment at TTT in the future, such as a revision of budget to purchase more secure portable devices and equipment.

The two meetings to discuss the InfoSec proposals facilitated the exchange of concerns and solutions between the project team, top management and the champions. Such exchange to discuss and achieve a consensus on InfoSec matters between top management and staff had not occurred before at TTT. The project team and top management now had a clearer understanding about the unique InfoSec issues and desired solutions of each department, while the champions acknowledged their critical role in the diffusion of InfoSec knowledge and understood their contributions were taken seriously. The meetings also enabled the project team to understand more about the challenge that some champions experienced, their lack of confidence in communication abilities, and devise two diffusion approaches to assist their diffusion. Specifically, the champions may conduct formal training sessions or informal discussions with their colleagues in the same departments. After the meetings the champions confirmed that they were now equipped with the necessary knowledge for the diffusion and suitable diffusion methods.

7.5 Reflection

The project team and top management considered this action taking stage as successful as the primary objectives to train the selected champions and have them diffuse InfoSec knowledge was met. The CAR project was agreed to progress to the next and final stage. The champions' lack of confidence in communication abilities was relevant to the objectives of the CAR project, which aimed at carrying out and studying the diffusion of InfoSec knowledge. It suggested that in addition to the champions' centrality in social networks, background characteristics and social interactions, which were identified in the previous action planning stage as important criteria for selecting the champions, organisational skills could also impact their potential to exert influence over others' InfoSec behaviours. On this basis, the meetings after the workshops with the champions to discuss their concerns were useful.

7.6 Chapter Summary

In the action taking stage discussed in this chapter, the project team jointly designed and conducted InfoSec training for the 50 champions identified in the previous stage. The training's

purpose was to prepare these champions for the diffusion of InfoSec knowledge. To this end, the relevant literature was reviewed and identified four key elements for successful InfoSec training—collaborative learning, critical reflection, relevancy and facilitating conditions—were identified. Of the various InfoSec training approaches, Karjalainen and Siponen (2011) suggested an experiential learning cycle-based InfoSec training approach which satisfied these four key elements through the provision of a step-by-step instruction on how to conduct InfoSec training. Some of the suggested activities had to be modified to make this training approach feasible in TTT's context.

Four workshops were conducted for the 50 champions, and the champions developed InfoSec proposals which detailed solutions to the InfoSec issues in their departments. The project team also discussed the champions' challenges which could affect the diffusion effectiveness. The project team, top management and the champions reached a consensus on two diffusion approaches. Specifically, champions diffusing InfoSec knowledge to colleagues in large departments could conduct formal training sessions, while diffusion for small departments could be in the form of informal discussions. Champions from the project management department also volunteered to prepare training materials for the diffusion.

At the end of this stage the champions had diffused the InfoSec knowledge to the colleagues in their departments. The next and final stage evaluated the improvements in the InfoSec-related socialisation and investigated the formation of an InfoSec climate in TTT. A summary of this stage's research activities is shown in Figure 7.5.

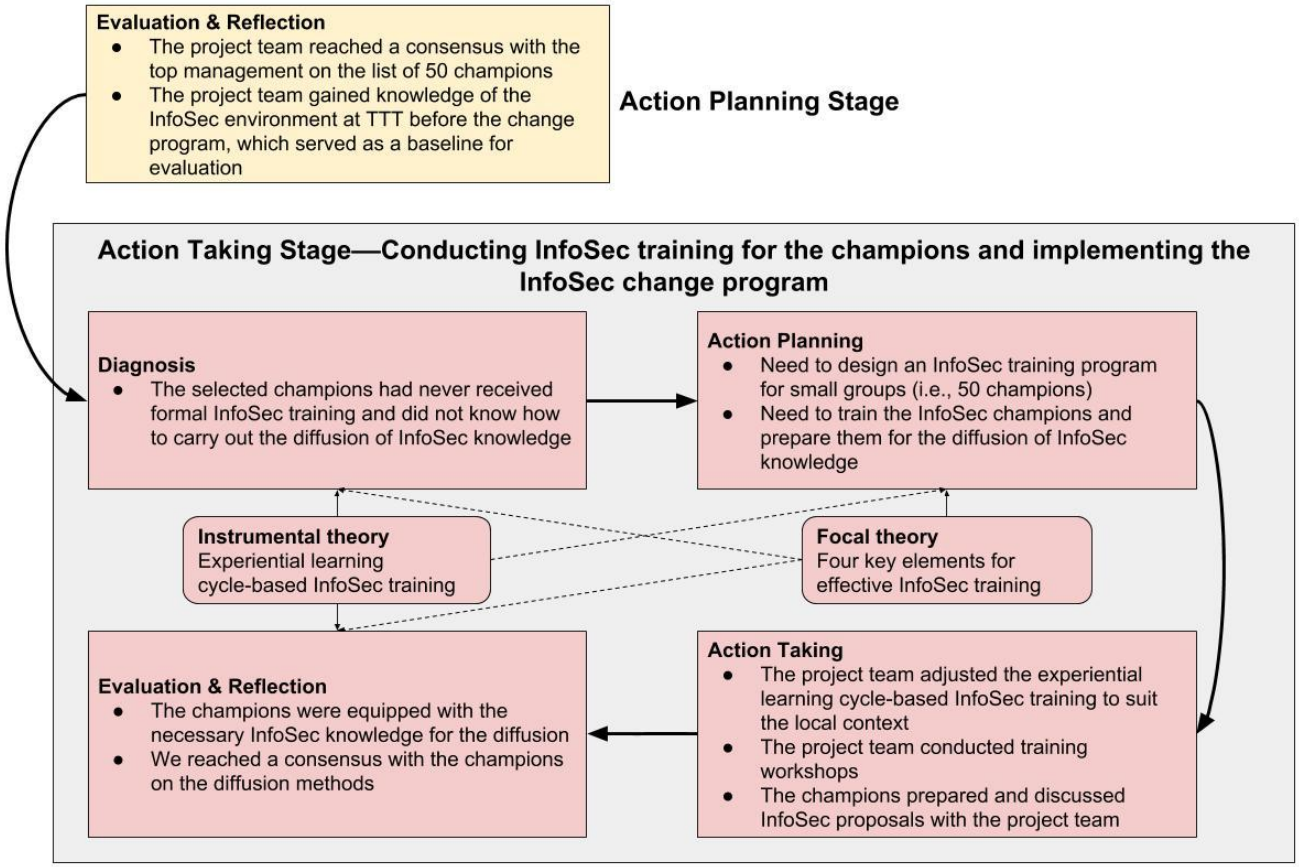


Figure 7.5. Summary of the Action Taking Stage

Chapter 8: Evaluation and Reflection Stage—Evaluating the InfoSec Change Program's Effectiveness

This chapter discusses the last evaluation and reflection stage of the CAR project. In the diagnosis section the objectives of the iteration were identified. These objectives were to evaluate the change program's effectiveness (the business objective) and to investigate the formation of an InfoSec climate (the scholarly objective). In the action planning section, I discussed the planned activities—collecting data by using the same questionnaire in the second iteration, performing a longitudinal SNA to examine the formation of an InfoSec climate, establishing the key performance indicators (KPIs) to evaluate the changes in the InfoSec-related networks and performing the evaluation. In the action taking section, these planned actions were carried out. The outcomes of these actions are reviewed in the evaluation and reflection sections. Figure 8.1 summarises the structure of this chapter.

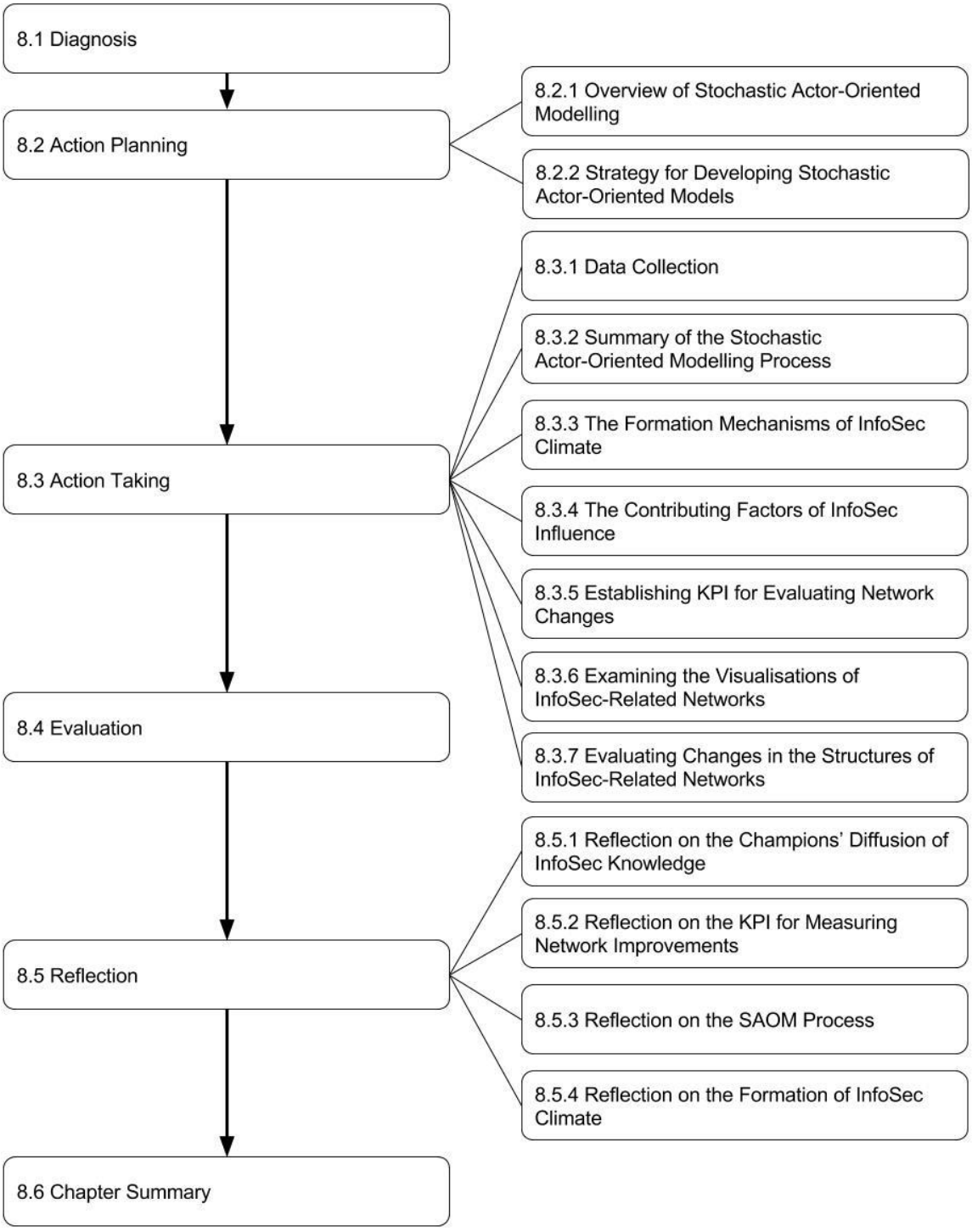


Figure 8.1. Structure of Chapter 8

8.1 Diagnosis

Through the first three stages I conducted a risk assessment at TTT and interviews with external InfoSec experts, a SNA to analyse the pre-intervention InfoSec-related networks and identify influential InfoSec champions, and trained champions for the diffusion of InfoSec knowledge

as part of the change program to enhance TTT's InfoSec environment. Subsequently, the champions performed the InfoSec diffusion for four months, top management launched an InfoSec competition event, employees hung InfoSec awareness posters and started to report InfoSec issues and the 'Locky' malware incident occurred.

Shortly before the champions' diffusion of InfoSec knowledge top management launched the initiative with a company-wide event to increase employees' InfoSec awareness and participation in InfoSec-related activities. A public announcement was posted on the company's Intranet portal which called for submissions of InfoSec vulnerabilities in the workplace. Once the project team received the submissions, the submitted InfoSec vulnerabilities were compared with those identified from the risk assessment and ranked according to their severity and novelty. The employee who submitted the top-ranked vulnerability and the department of that employee would be rewarded with a small amount of money (AUD 12 or VND 2 million). The top management explained that they launched the event to raise all employees' InfoSec awareness by encouraging them to pay attention to their surrounding workplace and seek InfoSec vulnerabilities. Top management also believed that such an event would raise employees' awareness of the company's InfoSec-related initiatives and potentially make them more receptive to the champions' InfoSec influences.

Many computers at TTT were also infected by a ransomware called 'Locky' seven days before the champions carried out the diffusion of InfoSec knowledge. This ransomware locked the work files on the computers and made them unusable until the victim agreed to pay the hacker a ransom. However, the IT and BSP departments made frequent backups of the company's work files and the locked files along with the ransomware could be safely removed. The project team observed that the occurrence of this 'Locky' malware incident made all employees at TTT recognise the real InfoSec threats that could happen to the company. During the diffusion the project team received numerous reports from employees and the champions about suspicious emails, most confirmed to contain viruses. Moreover, some employees voluntarily hung cartoons about InfoSec around the workplace (see Figure 8.2) to remind others about the importance of InfoSec.

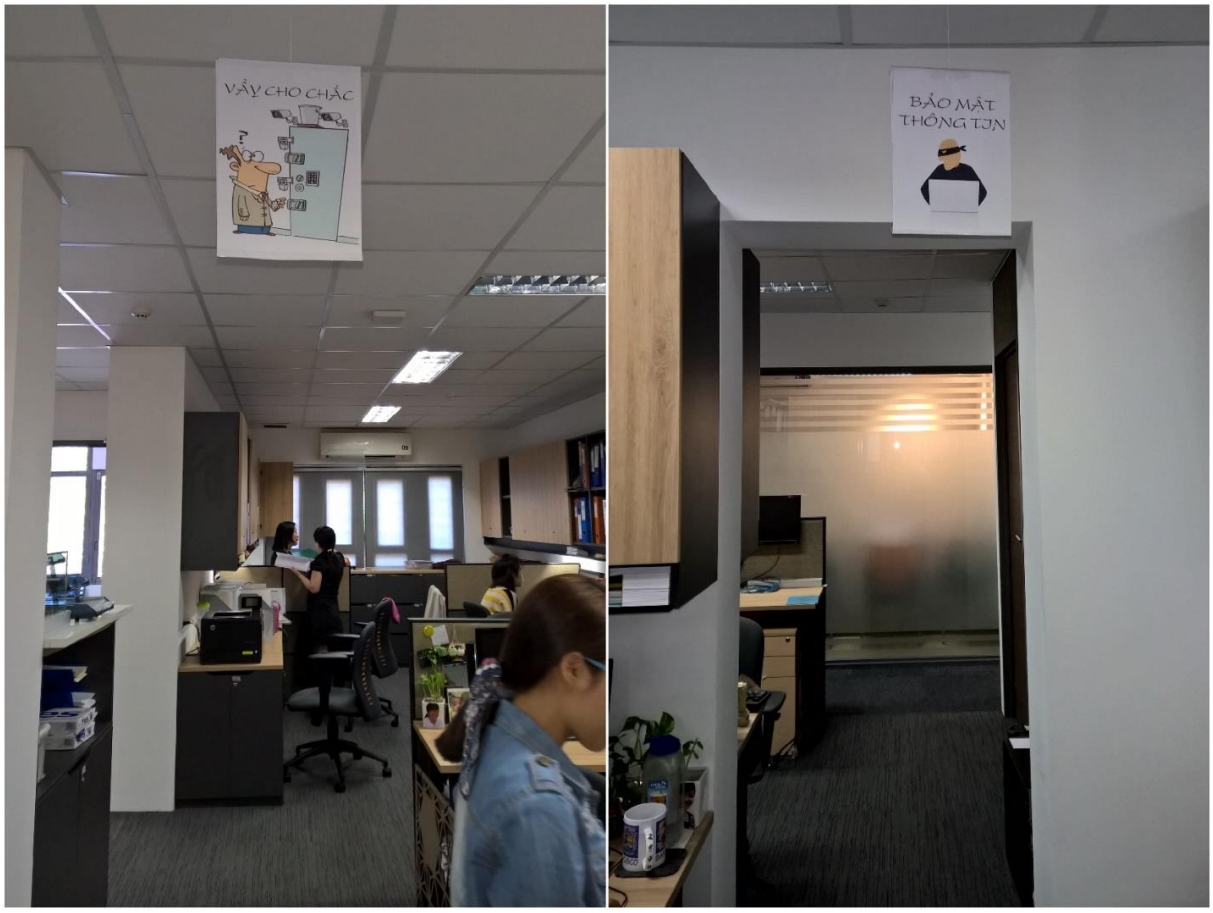


Figure 8.2. Cartoons to Raise InfoSec Awareness in the Workplace

The cartoon on the top left shows a man standing next to a locker with many locks and the Vietnamese message reads 'vầy cho chắc' or 'do like this to make sure' as a comical reminder to pay attention to protecting confidential information. The cartoon on the top right shows a hacker using a computer and the Vietnamese message reads 'bảo mật thông tin' or 'information security' to remind employees about InfoSec threats and the importance of InfoSec in the workplace.

The project team appreciated top management's launch of the InfoSec event and the voluntary action of employees in putting up cartoons as an indicator of their participation with genuine interest, rather than solely aiming at the performance of such action in terms of promoting InfoSec awareness. These events indicated an overall improvement in the InfoSec environment at TTT, but no formal evaluation of the outcome of the InfoSec diffusion and performance of the champions had yet been performed. The project team and top management at this point did not have any quantitative evidence that supported whether the diffusion had improved the InfoSec environment. Moreover, TTT did not have the KPIs for such an evaluation.

Thus, the objectives of the fourth and final stage of the project were to establish quantitative evidence, evaluate the outcome of the change program and identify the forming mechanisms of InfoSec climate. Together with the actions performed in the previous stages, considered as

successful by the project team and top management, an improved InfoSec environment and the identification of the forming mechanisms of this InfoSec climate would allow the conclusion of the CAR project.

8.2 Action Planning

The project team planned to perform two activities in this stage—identify the forming mechanisms of the InfoSec climate to meet the scholarly objective and evaluate the changes in the InfoSec-related networks at TTT after the change program. These planned activities required launching the same survey that had been used in the action planning stage (see Chapter 6) to collect data about employees' InfoSec-related interactions and climate perceptions after the change program, then applying SNA methods to examine the changes in these interactions and climate perceptions. As part of the activity to evaluate the changes in the InfoSec-related networks, the project team would also establish the KPIs of the improvements in the networks of InfoSec-related interactions.

Consistent with my scholarly motivation, I chose theories on the formation of an InfoSec climate (Ashforth 1985; Chan, Woon & Kankanhalli 2005; Schneider & Reichers 1983) as the focal theory for this stage. Employees' perceptions of InfoSec climate are formed as a result of their socialisation in the workplace, which facilitates the informational and normative influences that shape a shared understanding about InfoSec practices and priority (Ashforth 1985; Chan, Woon & Kankanhalli 2005).

In this project, employees' socialisation was represented by networks of the provisions of work-related advice and/or organisational updates, personal advice and/or trust in expertise and InfoSec advice and/or troubleshooting support. The impacts of the networks of employees' socialisation on the InfoSec influence network had been analysed in the action planning stage (see Chapter 6). In this stage I continued to analyse the relationships between employees' socialisation and InfoSec influence, and between InfoSec influence and the formation of employees' perceptions of InfoSec climate.

Leenders (2002) stated that social influence occurs when information is communicated from one actor to another actor, and the latter actor adjusts their behaviour, attitude, or belief to match the former actor's behaviour, attitude or belief in that social system. When performing SNA, the occurrence of social influence in a social network is hinted when researchers detect

clusters of nodes which are tied to each other and have similar attributes, since some of these nodes might have matched their attributes with other nodes of the same clusters. However, social influence still cannot be accurately claimed due to the homophily effect that can also result in a similar phenomenon. Mouw (2006) posited that, according to the principle of homophily (McPherson, Smith-Lovin & Cook 2001), people tend to purposely choose the people and social groups that they want to be associated with. Such purposive selection of nodes to connect with can also lead to the formation of clusters of nodes having similar attributes, but does not necessarily imply the occurrence of social influence. In such a situation, none of these nodes has changed their attributes to match with connected others—that is, social influence did not occur, they simply chose to connect with each other since they had similar attributes (i.e., homophily effect).

In this project's context, employees whose climate perceptions were already at an elevated level might have chosen to socialise with those whose levels of climate perceptions were also high. In that case, there is no evidence to suggest that employees' socialisation has modified their climate perceptions because of social influence. Such a phenomenon reflects the selection process that determines who people choose to socialise with based on their traits, rather than reflecting the changes in people's traits caused by their socialisation as an effect of social influence.

The central issue here focuses on empirically distinguishing the social influence and the selection process to truly understand the phenomenon, requiring longitudinal data that describe the changes in the nodes' attributes over time, from being at one level to another level as a result of the nodes' connections (Borgatti, Everett & Johnson 2013; Steglich, Snijders & Pearson 2010). Steglich, Snijders and Pearson (2010) addressed this issue by developing the SAOM method to simultaneously analyse selection and influence as two separate processes. Since its introduction, this method had been adopted by studies in research fields such as organisational behaviours (Wölfer & Scheithauer 2014), leadership (Emery, Daniloski & Hamby 2010), adolescents' behaviours (DeLay et al. 2016; Dijkstra et al. 2010; Fortuin, van Geel & Vedder 2015) and safety climate (Schulte, Cohen & Klein 2012). Performing SAOM utilises the data structures that represent network concepts of nodes and ties based on graph theory (Barnes & Harary 1983). As a result, I also used graph theory as the instrumental theory for this stage.

8.2.1 Overview of Stochastic Actor-Oriented Modelling

Performing SAOM involves specifying a model with terms that describe the mechanisms of network formation or dissolution and then evaluating that model. The SAOM method examines changes in the network by decomposing these changes into the mini-steps that occur between the points in time when the data is captured, where the employees represented by the nodes make a decision to maintain or change one outgoing tie based on their network position and attributes (Ripley et al. 2017). Based on the modelled terms that describe the mechanisms governing such a decision of the nodes to maintain or change their ties, the statistical procedures implemented in the SAOM method produces a probabilistic evolution of the network which shows how the network 'evolves' from one state to another (Ripley et al. 2017).

The SAOM method and its accompanying tool require nodal attributes to be in single integer form with values ideally deviating only within a range of up to five points (Ripley et al. 2017). Studies using SAOM examined binary variables that describe the respondent's behaviour (Dijkstra et al. 2010), whereas psychometric variables such as attitudes and perceptions were often averaged and rounded to integer (e.g., Caravita et al. 2014; Putzke et al. 2013; Rambaran, Dijkstra & Stark 2013). The process to compute InfoSec climate scores for the SAOM analysis is in Appendix E.

In line with prior studies on InfoSec climate (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013) and climate formation (Ashforth 1985; Schneider & Reichers 1983), the purpose of conducting a SAOM analysis in this stage was to identify the factors and mechanisms that contributed to the formation of InfoSec climate.

Employees' socialisation through the provisions of instrumental resources, expressive resources and InfoSec support was assumed to lead to InfoSec influence which would subsequently shape employees' climate perceptions. For this purpose, the major effect examined was the relationship between the number of InfoSec influencers who exerted InfoSec influence over employees and their climate perceptions. It was also assumed the occurrence of InfoSec influence and employees' climate perceptions would be both affected by employees' background characteristics as control variables. Figure 8.3 summarises the theoretical model examined through the SAOM method.

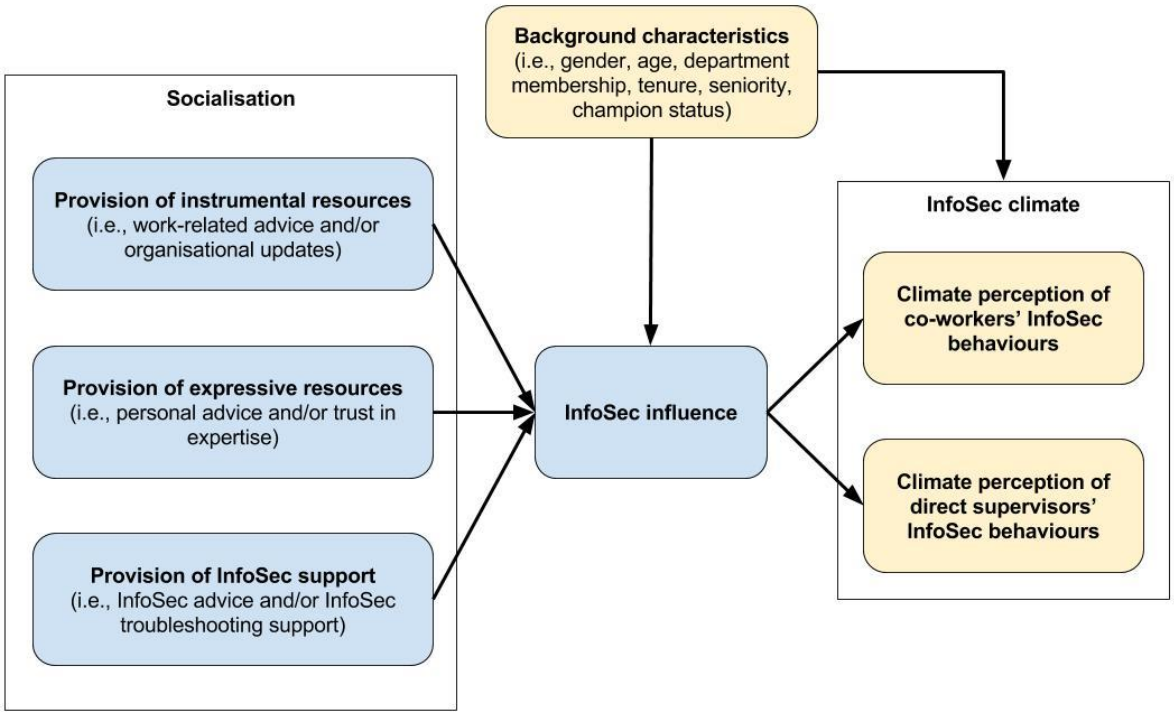


Figure 8.3. Theoretical Model

8.2.2 Strategy for Developing Stochastic Actor-Oriented Models

The impacts of employees' socialisation and background characteristics on exerting InfoSec influence (Sections 6.2.1 and 6.2.2) and the effects concerning the formation of network ties were discussed in the action planning stage (Chapter 6). When performing SAOM analysis, researchers may examine various social influence effects which belong to two major groups—the assimilation effects and the contagion effects (Steglich, Snijders & Pearson 2010). Assimilation effects refer to the phenomenon where an actor adjusts their perception score to be similar to those of other connected actors, whereas contagion effects describe an actor's tendency to increase their perception score when connecting with other actors whose perception scores are high (Ripley et al. 2017). Researchers can further determine whether the number of neighbours that the focal actor connects to can impact the assimilation and contagion effects. This leads to four possible social influence effects explained below.

In this project's context, the average assimilation effect models the likelihood that employees will change their climate perceptions to be similar to others from which they receive InfoSec influence ties. The average contagion effect models the likelihood that employees will increase their climate perception scores to a higher level as they are tied to other employees whose climate perception scores are high.

The influence mechanisms of matching and increasing climate perception scores were the same for the total assimilation and total contagion effects. The difference between the effects with the prefix 'average' and those with the prefix 'total' was that the former effects assumed employees' number of InfoSec influencers did not have any impact on social influence. In other words, the social influence effect on climate perceptions would be the same for all employees regardless of the total number of InfoSec influencers they had. The total assimilation and total contagion effects both assumed that employees' total number of InfoSec influencers determined the social influence effects on their climate perceptions. The formal definitions of the four social influence effects and their descriptions are provided in Table 8.1.

Table 8.1. Social Influence Effects in Stochastic Actor-Oriented Modelling

	Neighbours' average perceptions	**Neighbours' total perceptions**
Assimilation	$x_{i+}^{-1}\sum_j x_{ij}\left(sim_{ij}^{z} - \widehat{sim^{z}}\right)$ Purpose: modelling the likelihood that actor *i* adjusts their perception score *z* to match with those of actor *j* who they are tied to	$\sum_j x_{ij}\left(sim_{ij}^{z} - \widehat{sim^{z}}\right)$ Purpose: modelling the likelihood that actor *i* adjusts their perception score *z* to match with those of actor *j* who they are tied to (actor *i's* total number of connected actors impacts assimilation effect)
Contagion	$z_i\left(\sum_j x_{ij}\, z_j\right) / \left(\sum_j x_{ij}\right)$ Purpose: modelling the likelihood that actor *i* increases their perception score *z* as they are tied to actor *j* whose perception scores are high	$z_i\left(\sum_j x_{ij}\, z_j\right)$ Purpose: modelling the likelihood that actor *i* increases their perception *z* as they are tied to actor *j* whose perception scores are high (actor *i's* total number of connected actors impacts contagion effect)

Researchers may choose to include any social influence effects in a stochastic actor-oriented (SAO) model based on theoretical justifications (Ripley et al. 2017). Ripley et al. (2017) also recommended that researchers may employ a backward selection approach which involves performing analyses on all social influence effects and retaining the effects that achieved statistical significance. However, Ripley et al. (2017) cautioned that including many social influence effects in one model could lead to multicollinearity i.e., having multiple predictors of an outcome that are highly correlated and non-convergence, meaning that the model fails to arrive at a conclusive outcome with reliable results.

A statistically significant and positive contagion effect implied that employees together developed favourable climate perceptions through social influence. A significant and positive assimilation effect implied that employees received influences from other employees then

matched their climate perceptions which became either more favourable or more unfavourable. An InfoSec climate formed when employees have their climate perceptions influenced by others (Ashforth 1985) regardless of the influenced perceptions' nature being favourable or unfavourable (i.e., a high or low score). Thus, confirmation of any of the social influence effects listed in Table 8.1 would provide evidence for the formation of an InfoSec climate caused by social influence.

Since the InfoSec change program aimed at improving employees' climate perceptions, the confirmation of a contagion effect was desired more than confirming an assimilation effect in TTT's context. Therefore, I prioritised the estimation of the average contagion and total contagion effects in this stage. Moreover, I used the weighted version of these effects which emphasised the InfoSec influence exerted among employees in the same departments. This modelling decision was consistent with the InfoSec climate questions in the survey (see Table 6.2) and the theoretical scope of climate perceptions which focused on the colleagues and the direct supervisors of the respondents (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013).

In summary, the plan for this stage was to perform the longitudinal SAOM analysis to identify the mechanisms and factors that contributed to the formation of an InfoSec climate, as shown in the theoretical model in Figure 8.3. The SAOM analysis required the collection of data about the networks and employees' climate perceptions after the change program by launching the questionnaire used in the action planning stage. In line with TTT's business objective, the project team would establish the KPIs of the changes in the InfoSec-related networks and perform the evaluation based on these KPIs.

8.3 Action Taking

Consistent with the action plan the project team carried out the SNA to perform the two key research activities in this stage—examining the formation of InfoSec climate by performing SAOM analysis and evaluating the changes in the InfoSec support and InfoSec influence networks. Data collection was performed to support the first activity and the project team established the KPIs to support the second activity.

8.3.1 Data Collection

The same questionnaire used in the action planning stage was launched after the four-month diffusion of InfoSec knowledge by the champions. To minimise common method bias the following remedies were employed in the design of the questionnaire. I mixed the order of questions to avoid sequences of questions that belonged to the same construct and included detailed definitions and examples to clarify any potentially vague questions (Podsakoff et al. 2003). The questions about networks and employees' perceptions of InfoSec climate are in Tables 6.1 and 6.2 in Chapter 6. Employees' background characteristics (i.e., gender, age, tenure, seniority and department membership) were extracted from the HR database that contained information about all employees at the time of data collection.

Missing data is problematic for longitudinal network research as it can lead to biased results without a thoughtful treatment (Ripley et al. 2017). The whole-network design of network research, which focuses on all individuals within a bounded community, is especially prone to the risk of having missing data as members of a bounded community such as TTT can enter or exit the network between the different points in time of the network analysis (Borgatti, Everett & Johnson 2013). Additionally, some respondents who previously participated in the research may refuse to participate in a survey collecting network data at a later point. In this context, it is worth mentioning that the competitive construction industry in Vietnam has a high turnover rate and employees often change firms. The project team was affected by such turnover effects and the respondents' refusals, collecting 230 responses from the survey in this stage compared to 264 responses from the previous survey. Specifically, 23 employees left TTT during the diffusion period. Of the 311 employees available at the time when the previous survey was launched, 47 refused to answer the questionnaire (response rate of 85%). In this stage, 58 of 288 employees refused to participate in the survey (response rate of 80%).

The project team, therefore, decided to only select those employees who had cast their nominations at both points in time for further analysis. This resulted in a dataset of 152 employees. Employees who held central positions in the networks such as the IT and BSP employees and the 40 remaining champions (10 had left TTT before the second survey was launched) were available in this dataset. The removed nodes possessed relatively few ties and held peripheral positions; their removals did not significantly affect the nature of the networks.

8.3.2 Summary of the Stochastic Actor-Oriented Modelling Process

I analysed the SAO models by using the R package named 'RSiena' (version 1.1-307, released 12 May 2017) (Ripley et al. 2017), the most developed software package for performing SAOM at this time. I computed in the R programming environment the Moran's I coefficients which measured the similarity in employees' perceptions of colleagues' and direct supervisors' InfoSec behaviours. Before the change program, Moran's I coefficients of employees' climate perceptions of colleagues' and direct supervisors' InfoSec behaviours were –0.08 and –0.03 respectively. After the change program, perceptions of colleagues' InfoSec behaviours had a Moran's I coefficient of 0.07 while perceptions of direct supervisors' InfoSec behaviours had a Moran's I coefficients of 0.06. The negative values of Moran's I coefficients before the change program and positive values post-program indicated that the InfoSec influencers and influenced employees had dissimilar perceptions before the change program, but these perceptions became more similar after the change program.

Next, the Jaccard index indicates the stability of the networks over time (Ripley et al. 2017). Ripley et al. (2017) advised that Jaccard indices of 0.3 and above are desirable for the estimation process while indices of below 0.1 indicate that performing SAOM on the dataset is not advisable. For my dataset, the computed Jaccard index of 0.195 was not above the desirable value, but it was not too problematic either.

Consistent with the modelling strategy, I analysed four SAO models to explain the formation of an InfoSec climate by InfoSec influence, which consisted of two contagion models and two assimilation models. These four models all had the same effects which described the network dynamics (i.e., the forming mechanisms of InfoSec influence ties). The effects that described the perception dynamics (i.e., the four types of social influence effects) and the features of climate perceptions were modelled separately for each of the four models. The detailed modelling process is described in Appendix F. This section summarises the key results of the SAO models with regard to how employees formed their climate perceptions as they received InfoSec influence from their colleagues in the same departments.

I started with analysing the *average contagion model* which posited that employees increased their climate perception scores as they received InfoSec influence from colleagues in the same department, whose climate perception scores were also high. This model assumed that such social influence effect would occur for all employees regardless of the number of colleagues

who exerted InfoSec influence over them. The results of this model indicated that such a phenomenon did not occur. This outcome led me to explore an alternative explanation which assumed that employees' total number of InfoSec influencers could govern the social influence effect.

I performed the analysis for the *total contagion model* with such an assumption. This model's results indicated that employees increased the scores of their climate perceptions of colleagues' InfoSec behaviours as they received InfoSec influence from many colleagues in the same department. However, the results did not confirm the same phenomenon for employees' climate perceptions of direct supervisors' InfoSec behaviours. An unusually large standard error of the total contagion effect also suggested that the analysis might have had issues and the effect should be re-analysed by using the score test (Ripley et al. 2017). I followed Ripley et al.'s (2017) recommendation and performed a score test for the total contagion effect on employees' climate perceptions of colleagues' InfoSec behaviours. The score-tested model did not have any issues, and the results reinforced that the total contagion effect only affected employees' climate perceptions of colleagues' InfoSec behaviours, but not the climate perceptions of direct supervisors' InfoSec behaviours.

I continued to explore the assimilation effects which posited that employees matched their climate perception scores with those of other employees from which they received InfoSec influence. If the assimilation models confirmed that the average assimilation and total assimilation effects also affected only employees' climate perceptions of their colleagues' InfoSec behaviours, then such results would reinforce results of the previous contagion models.

Since the total contagion model had confirmed the impact of employees' total number of InfoSec influencers on social influence, I started with analysing the total assimilation effect. The *total assimilation model* showed many issues and, therefore, its initial results could not be interpreted (see Figure F.2 in Appendix F). However, applying the score test resulted in a successful analysis of the model with no issues. The score test also confirmed that the total assimilation effect only affected employees' climate perceptions of colleagues' InfoSec behaviours, but not of direct supervisors' InfoSec behaviours, reinforcing the previous findings of the total contagion model.

The fourth model, *average assimilation model*, was analysed to validate the effect of employees' total number of InfoSec influencers on social influence. I applied the score test

again to analyse the average assimilation effect. Results of the score-tested average assimilation model indicated that social influence did not affect employees' climate perceptions when the number of their InfoSec influencers was not accounted for.

8.3.3 The Formation Mechanisms of InfoSec Climate

Results from the four SAO models confirmed that employees' total number of InfoSec influencers governed both the contagion and assimilation effects. When employees had many InfoSec influencers in the same department, they would develop more favourable climate perceptions of colleagues' InfoSec behaviours to match with those of the InfoSec influencers which were also favourable. SAOM analysis also revealed the natural tendencies of employees' climate perceptions of colleagues' and direct supervisors' InfoSec behaviours through results of the linear shape and quadratic shape effects (Ripley et al. 2017).

The linear shape effect expressed the tendency of employees' climate perception scores to increase over time. Only employees' climate perceptions of direct supervisors' InfoSec behaviours had significant and positive linear shape effects across the four SAO models. These results implied that employees tended to increase their scores of climate perceptions of direct supervisors' InfoSec behaviours over time. The linear shape effects of employees' climate perceptions of colleagues' InfoSec behaviours were non-significant in all models, which indicated that there were no patterns in the changing directions of these perceptions.

The quadratic shape effect described the adjustments of the perception scores. I found that employees' climate perceptions of colleagues' and direct supervisors' InfoSec behaviours had significant and negative quadratic shape effects in all four SAO models. These negative quadratic shape effects suggested that employees, whose climate perceptions were less favourable, tended to develop more favourable climate perceptions over time. Moreover, those who developed favourable perceptions would decrease their climate perception scores to be near the mean score.

Overall, the key forming mechanisms of InfoSec climate perceptions were as follows. First, employees' scores of their climate perceptions of colleagues' InfoSec behaviours tended to increase over time, but only when their previous climate perception scores were low or when they had many InfoSec influencers in the same department. This tendency was different from that of employees' climate perceptions of direct supervisors' InfoSec behaviours, which would increase perception scores regardless of the previous scores or the number of InfoSec

influencers. In any case, employees' tendency to develop both climate perceptions to become more favourable over time, which implied that the InfoSec climate at TTT had been improved. Second, when employees' climate perception scores were too low or too high, employees would adjust their climate perceptions accordingly by increasing or decreasing the scores. This implied that climate perceptions were likely to be governed by group norms that favoured the formation of consensus rather than developing polarising climate perceptions.

8.3.4 The Contributing Factors of InfoSec Influence

The results of the four SAO models confirmed that employees increased the scores of their climate perceptions of colleagues' InfoSec behaviours as they received InfoSec influence from many other employees in the same departments. Thus, it was important to identify the factors that increased the number of InfoSec influencers.

The SAO models' results indicated that employees rarely received InfoSec influence from other employees, and the InfoSec influence network did not have any specific patterns with regard to the reciprocal exerting InfoSec influence. The rate effect of changing the number of InfoSec influencers over time was relatively high which implied that the InfoSec influence network had been profoundly altered after the change program.

The significant and positive transitivity effect indicated that the InfoSec influence network was transitive, or that employees were more likely to directly receive InfoSec influence from those who indirectly exerted InfoSec influence over them. The in-degree popularity and out-degree popularity effects expressed employees' tendency to increase both received and exerted InfoSec influence from and over other employees over time. As both effects were positive and significant across the four SAO models, they suggested that influential employees tended to become more influential and influenced employees were influenced more by colleagues through the change program. Since a KPI of the change program was to facilitate InfoSec influence through the champions' diffusion, these results provided the evidence that supported the change program's success.

Among the effects of employees' background characteristics on InfoSec influence that were included in the four SAO models, the results only confirmed the effects of employees' department membership and champion status. Specifically, employees who worked in the same departments tended to exert InfoSec influence over each other. Employees who were champions also tended to exert InfoSec influence over more people compared to non-champion

employees. All results of the effects mentioned so far, except the effect of champion status which had not been previously tested, were consistent with those found in the ERGM analysis in the action planning stage (see Chapter 6). The confirmed positive effect of champion status on the tendency of exerting InfoSec influence suggested that the champions had emerged as new sources of InfoSec influence after the change program.

The out-in degree assortativity effect expresses the tendency of network actors with high out-degrees to have ties to other actors with high in-degrees (Ripley et al. 2017). In the context of this project, the effect modelled the phenomenon where employees, who received InfoSec influence ties from many other employees, would be more likely to receive InfoSec influence ties from overly influential employees such as the IT or BSP staff. The results indicated that such a phenomenon would be less likely to occur. In other words, employees who already had their InfoSec behaviours influenced by many other employees would not receive InfoSec influence from overly influential employees. Since the other result indicated that the champions were more likely to exert InfoSec influence over time, interpreting these results together suggested that employees had received less InfoSec influence from the IT or BSP staff and more InfoSec influence from the champions. This served as further evidence of the success of the change program.

The in-degree structural equivalence effect describes the tendency of network actors with similar in-degrees to be tied to each other (Ripley et al. 2017). I included this effect in the SAO models to capture the phenomenon where influential employees received InfoSec influence from each other, such as between the IT and BSP employees. Since the InfoSec influence network at TTT had only a handful of overly influential employees, including this effect in the models would allow a more accurate description of the observed network and add rigour to the models' results. Consistent with the observed structure of the InfoSec influence network, the results confirmed the positive likelihood of such a phenomenon.

I also examined the effects caused by employees' similar climate perceptions on exerting InfoSec influence. The results indicated that having similar climate perception scores did not impact exerting InfoSec influence. This finding reinforced the social influence effects that employees received InfoSec influence and subsequently increased their climate perceptions scores, rather than having similarly high climate perception scores and then purposively choosing to receive InfoSec influence from each other (see the discussion about selection and influence processes in Section 8.2.2).

Finally, the positive effects of employees' socialisation through their provisions of instrumental, expressive and InfoSec support resources on exerting InfoSec influence were confirmed across all four SAO models. The results indicated that employees tended to receive InfoSec influence from those who provided them with work and personal advice, organisational updates, InfoSec advice and InfoSec troubleshooting support and those whose expertise they trusted. Since the champions were tasked to diffuse InfoSec knowledge (i.e., give InfoSec advice to other employees), their active diffusion may have enabled them to exert InfoSec influence over other employees. Table 8.2 summarises the SAOM findings concerning the formation of employees' climate perceptions and the InfoSec influence as the main forming mechanism of the InfoSec climate.

Table 8.2. Summary of Stochastic Actor-Oriented Modelling Findings

Theoretical components	Findings
Climate perception of colleagues' InfoSec behaviours	• Became more favourable when receiving InfoSec influence from *many* InfoSec influencers in the same department, *whose climate perceptions were favourable* • Tended to become favourable over time • Self-regulated to become *less/more* favourable when current perception was *too favourable/unfavourable* • Unaffected by employees' gender, age, tenure, seniority and champion status
Climate perception of colleagues' InfoSec behaviours	• Unaffected by InfoSec influence • Self-regulated to become *less/more* favourable when current perception was *too favourable/unfavourable* • Unaffected by employees' gender, age, tenure, seniority and champion status
InfoSec influence	• Contributed to the formation of climate perception of colleagues' InfoSec behaviours • Rarely occurred between employees • Co-occurred with employees' socialisation i.e., provisions of instrumental resources/expressive resources/InfoSec support • Had transitive nature i.e., employees increased the likelihood to exert InfoSec influence over each other when there were multiple InfoSec influencers between them • Influencers became more influential over time; influenced employees received more influence over time • The likelihood to exert InfoSec influence increased between employees of the same departments • Champions had higher likelihood to exert InfoSec influence than non-champions • The likelihood to exert InfoSec influence was unaffected by gender, age, tenure, seniority and climate perceptions of colleagues' and direct supervisors' InfoSec behaviours

8.3.5 Establishing KPIs for Evaluating Network Changes

As part of the planned activities the project team established KPIs to evaluate the effectiveness of the champions' diffusion of InfoSec knowledge. Some of these KPIs—density, average

degrees, out-degree centralisation, reciprocity and transitivity—were selected since they had been evaluated in the action planning stage. The networks to be evaluated for those statistics were the InfoSec support and InfoSec influence networks.

Network density and degree centrality are often used to assess organisational information sharing where increases in these statistics imply active sharing (Hatala & Lutta 2009). To make sure every employee in the workplace has access to information after an intervention, Cross et al. (2004) recommended examining the distribution of ties (i.e., centralisation) and the core/periphery patterns that show the intended 'go-to' actors that are actually sought by others for advice.

More recently, Gesell, Barkin and Valente (2013) published the Network Diagnostic Tool which lists the meaningful network statistics to evaluate the effectiveness of an intervention and the recommended thresholds for these statistics. In addition to the common measures such as density, centralisation and number of ties (i.e., network actors' degrees) which were employed by prior studies, Gesell, Barkin and Valente (2013) suggested measuring the network's reciprocity and transitivity before and after the intervention. Reciprocity describes the ratio of mutual transmissions that reflect strong ties and transitivity measures cohesion in a network, and a high level of these two measures indicates that resources can be transferred well in the network (Gesell, Barkin & Valente 2013).

The project team decided that the change program would be considered as successful if the InfoSec-related networks' density, average degrees, reciprocity and transitivity increased after the change program. As the change program focused on diffusing InfoSec knowledge to all employees at TTT, the increased density, average degrees, reciprocity and transitivity of the InfoSec support network would indicate that there were more ties in the network post-program, which represented more provisions of InfoSec support after the change program. Likewise, the increases of these statistics for the InfoSec influence network would indicate that there were more opportunities for employees to receive the influence which improved their InfoSec behaviours.

In addition to measuring the networks' overall density, the project team measured within-department densities which evaluated the internal InfoSec-related socialisation between employees in the same departments. The increases of both the overall density and within-department density would indicate that employees not only elevated their provisions of InfoSec

support and InfoSec influence across departments, but also within their own departments. Specifically, employees would be more exposed to new knowledge if they received more external InfoSec support and InfoSec influence from other employees who worked in different departments. Moreover, increasing internal provisions of InfoSec support would mean that employees had access to more immediate and relevant InfoSec advice and InfoSec troubleshooting support from their colleagues in the same department. The increased exertion of InfoSec influence between members of the same department would also imply that consistent InfoSec climate and InfoSec behaviours could be reinforced and maintained within the departments. Thus, the project team decided on the increased overall density and within-department density of the InfoSec-related networks as the desired outcomes of the change program.

With regard to the number of outgoing ties or out-degrees of the network actors, the project team evaluated the out-degrees of all departments including the IT and BSP departments and of the champions. These out-degrees represented the number of employees who reported to have received InfoSec support and InfoSec influence from the departments and the champions. Specifically, the project team anticipated that the out-degrees of all departments except the IT and BSP departments would increase, which reflected that the departments had become more active in providing InfoSec support and exerting InfoSec influence. Similarly, the champions' out-degrees should also increase, indicating the champions had carried out the diffusion well. The out-degrees of the IT and BSP departments should decrease, which was in line with the change program's objective to decentralise the IT and BSP employees in the InfoSec support and InfoSec influence networks.

To evaluate the decentralisation of the overly influential IT and BSP employees, the project team measured the out-degree centralisation and transitivity statistics of the InfoSec-related networks. As high out-degree centralisation measures expressed high variations in the levels of providing InfoSec support and exerting InfoSec influence, a successful decentralisation would have such variations reduced (i.e., lower out-degree centralisation). A high transitivity measure in this project's context described the degree to which employees clustered together in groups that circulated InfoSec support and InfoSec influence. Higher levels of transitivity also indicated that the networks are less hierarchical (Gesell, Barkin & Valente 2013). As such, the project team decided the desired outcomes of the InfoSec-related networks to have lower out-degree centralisation and higher transitivity. The network measures as KPIs of the change

program, their desired outcomes and the meanings of these outcomes are summarised in Table 8.3.

Table 8.3. KPIs to Evaluate Changes in the InfoSec Support and InfoSec Influence Networks

KPI	Desired outcome	Meaning of outcome	Recommending sources
Density (whole network)	Increased	There are more provisions of InfoSec support and exerting InfoSec influence in the network.	Cross et al. (2004); Gesell, Barkin and Valente (2013); Hatala and Lutta (2009); Parise (2007); Valente et al. (2015)
Density (within department)	Increased	There are more provisions of InfoSec support and exerting InfoSec influence within departments.	Decided by project team
Average degrees	Increased	An employee provides more InfoSec support and exerts more InfoSec influence on average.	Hatala and Lutta (2009)
Out-degree (department)	Increased	Departments provide each other more InfoSec support and exert more InfoSec influence.	Decided by project team
Out-degree (champion)	Increased	Champions provide more InfoSec support and exert more InfoSec influence.	Decided by project team
Out-degree (IT and BSP departments)	Decreased	IT and BSP departments provide less InfoSec support and exert less InfoSec influence.	Decided by project team
Out-degree centralisation	Decreased	InfoSec support and InfoSec influence networks are not hierarchical and not dominated by a handful of employees.	Gesell, Barkin and Valente (2013); Valente et al. (2015)
Reciprocity	Increased	There are more mutual provisions of InfoSec support and exerting InfoSec influence between employees.	Cross et al. (2004); Gesell, Barkin and Valente (2013); Valente et al. (2015)
Transitivity	Increased	The provisions of InfoSec support and exerting InfoSec influence are more transitive; triads or three-node sets are brought together more.	Gesell, Barkin and Valente (2013); Valente et al. (2015)

8.3.6 Examining the Visualisations of InfoSec-Related Networks

The second major research activity of this stage was to evaluate the changes in the InfoSec-related networks and produce the quantitative evidence to assess whether the change program was successful. To evaluate the effectiveness of the change program, which involved the champions' diffusion of InfoSec knowledge, the project team examined the visualisations of

the networks before and after the change program. Subsequently, quantitative measures of the changes in the network structures were evaluated.

The large number of joiners and leavers at TTT drastically changed the population of employees from 311 to 288. Since the samples drawn from the time periods contained both old and new members, the project team considered that it would be less meaningful to evaluate the change program by including those who had been exposed to the change program but had already left, and those who had joined but had not been exposed to the change program. Therefore, to arrive at an accurate evaluation of the change program's effectiveness, we compared the InfoSec support and InfoSec influence networks that consisted of the 152 respondents who had participated in both surveys launched before and after the change program in the action planning and evaluation and reflection stages. These 152 employees were all exposed to the effects of the change program commenced in the action taking stage and were still working in TTT after the four-month diffusion of InfoSec knowledge.

The InfoSec support and InfoSec influence networks before and after the change program are depicted in Figures 8.4 to 8.7. The sizes of the nodes' labels are proportional to their out-degree centrality, which represent employees who were nominated as providers of InfoSec support or InfoSec influencers. The colours denote the nodes' department membership and the sources where the ties are sent from. Nodes with a letter '(C)' in their labels represent the appointed champions.

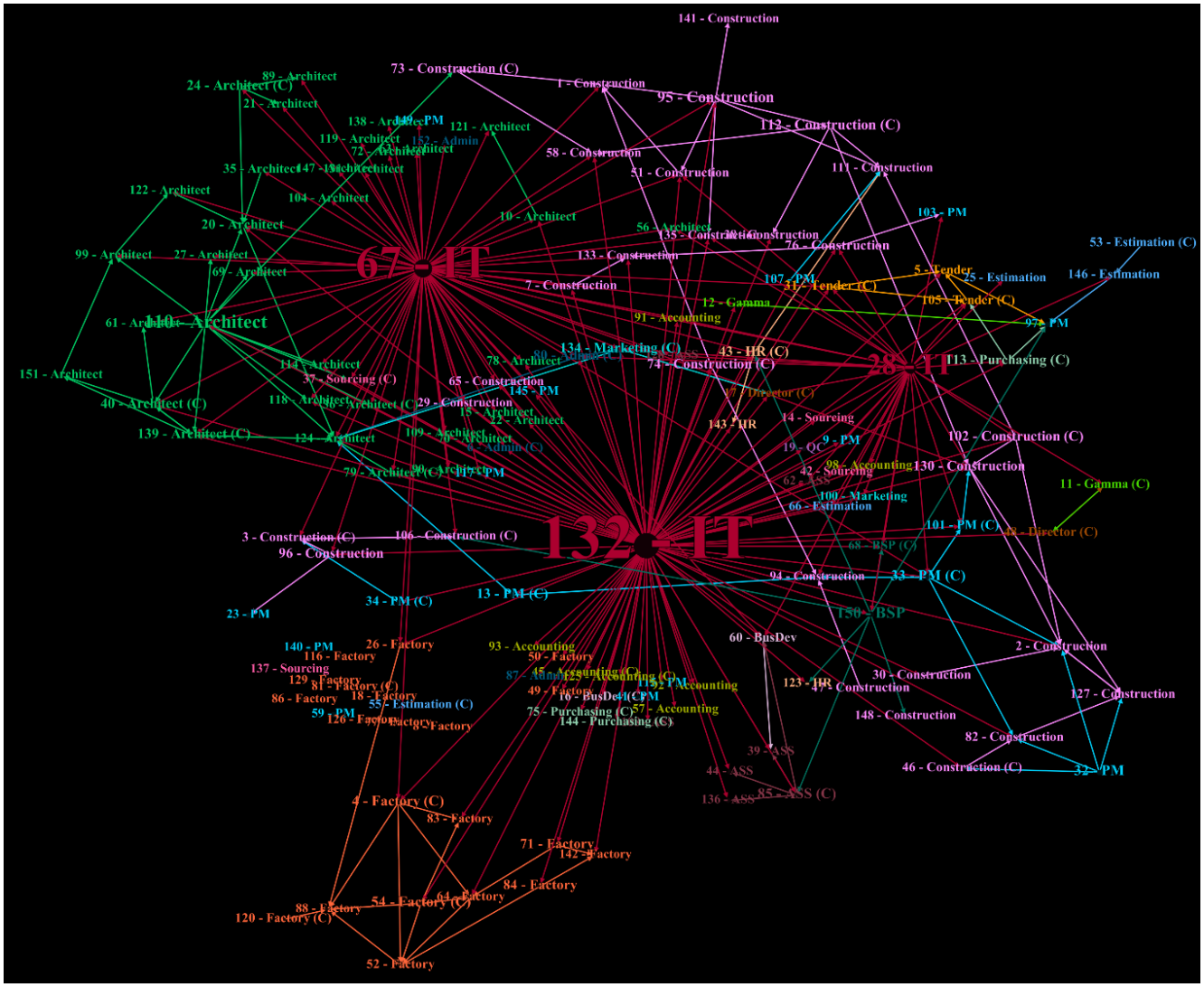


Figure 8.4. InfoSec Support Network before the Change Program

The InfoSec support network before the change program was almost completely controlled by three IT employees (note the comparatively larger label sizes in Figure 8.4). Consequently, the network did not appear to have any distinctive clusters except for the factory and architect departments, and most employees were tied to the IT staff as the central sources of InfoSec support.

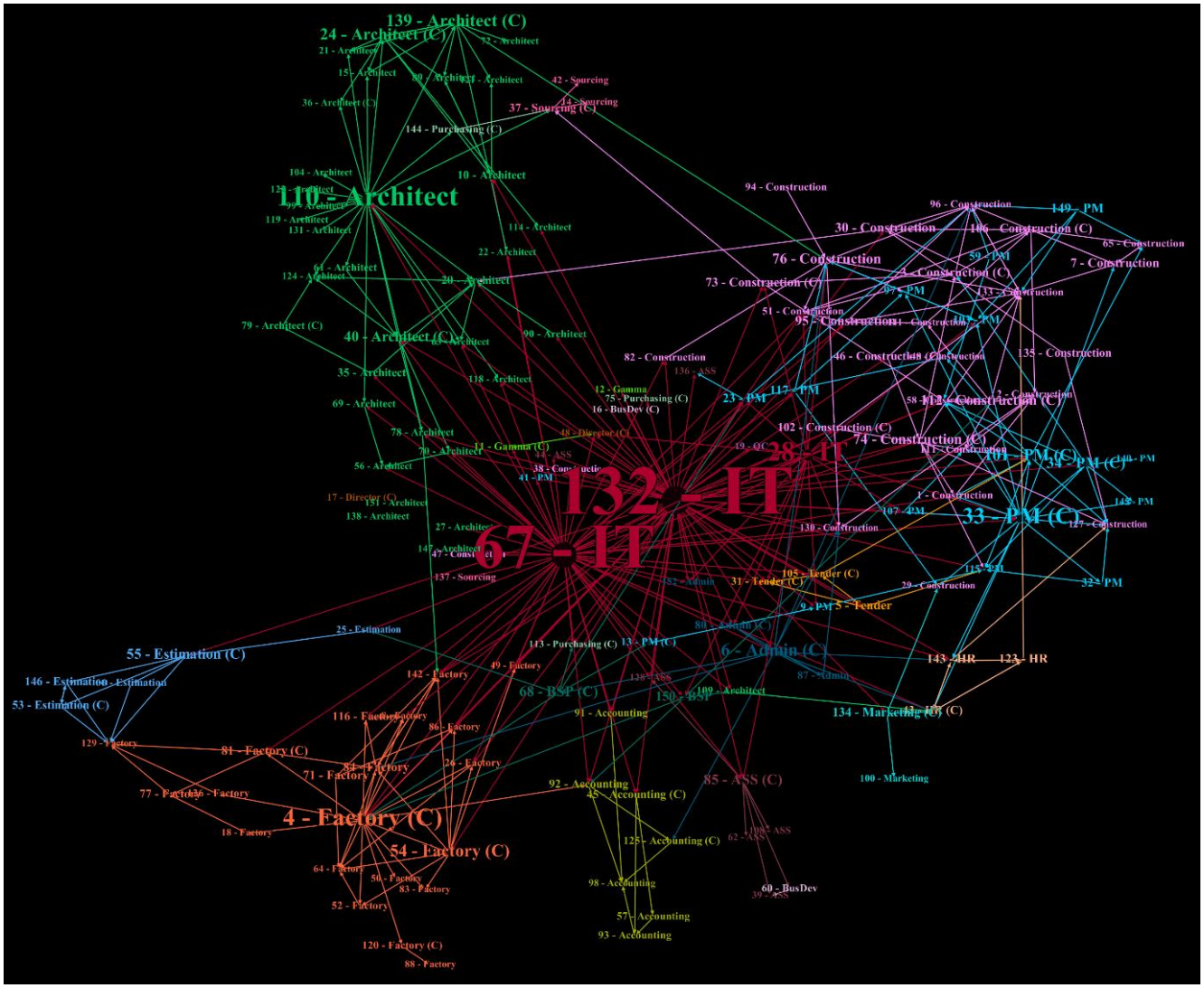


Figure 8.5. InfoSec Support Network after the Change Program

The InfoSec support network after the change program displayed considerable changes. There were more non-IT employees who emerged from their department as new central hubs of InfoSec support such as employee #4 from the factory department, employees #110 and #139 from the architect department, employee #33 from the project management department and employee #6 from the administration department. The new non-IT central sources were members of the newly formed large clusters in these departments which were distinctively visible. The formation of these clusters indicated that employees now had access to more immediate and relevant InfoSec support from local hubs beyond the IT employees, although the IT employees still held their active role in providing InfoSec support to other employees. The project team and top management considered the emergence of new sources as an enhancement of the InfoSec environment compared to the situation before the change.

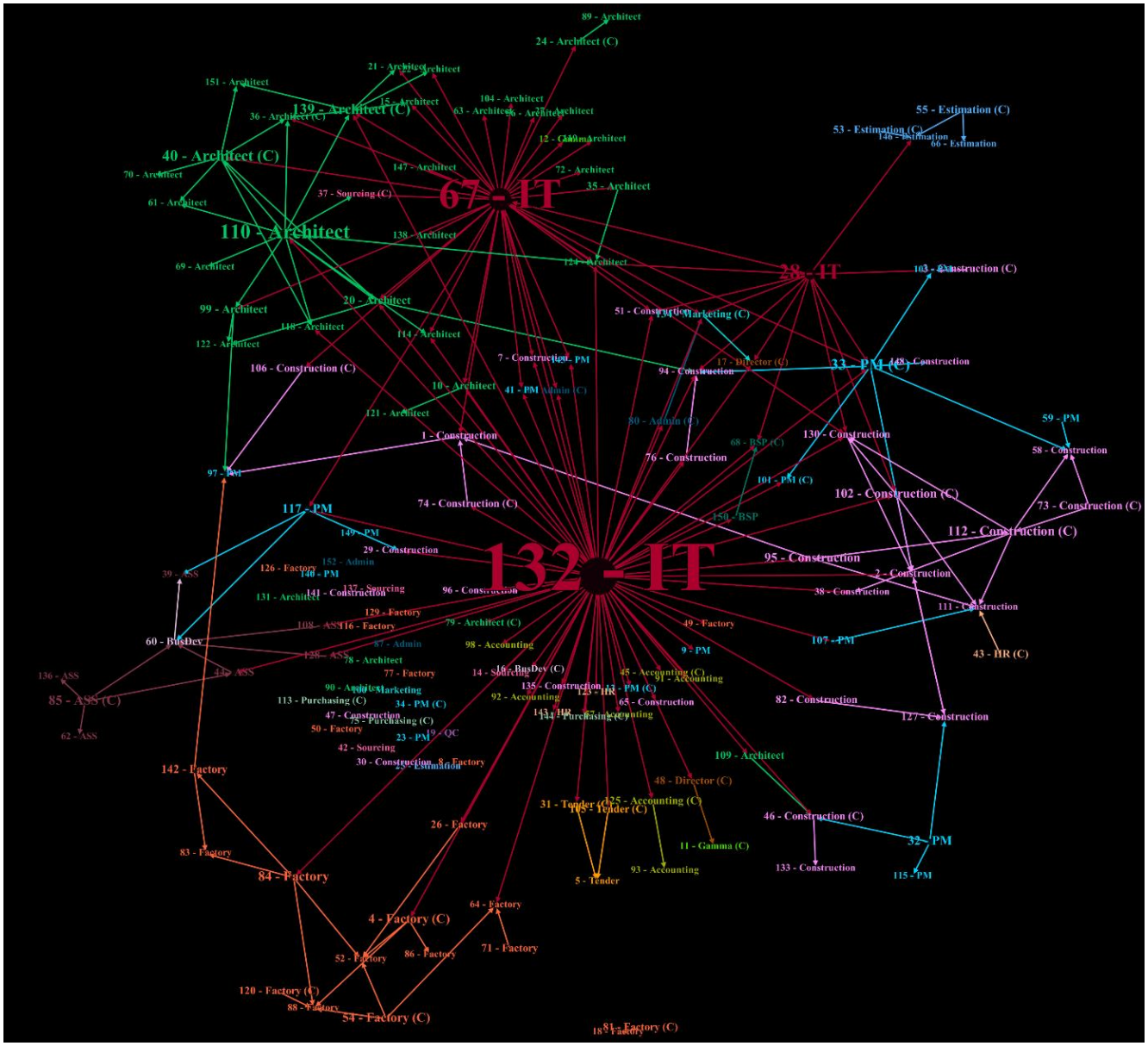


Figure 8.6. InfoSec Influence Network before the Change Program

The InfoSec influence network before the change program had a sparse structure dominated by the IT employees. It resembled the InfoSec support network before the change program. However, there were only two IT employees, #132 and #67 (instead of three in the InfoSec support network), who controlled the InfoSec influence network. These two IT employees lost some of their influence after the change program. The InfoSec influence network after the change program, as visualised in Figure 8.7, clearly shows the appearance of new sources of InfoSec influence in the project management and architect departments. The number of ties between non-IT employees had also increased (e.g., within the architect department and between the project management and construction departments) and had created new social

cliques (e.g., the estimation department). The project team and top management considered these changes as improvements in the InfoSec influence network.

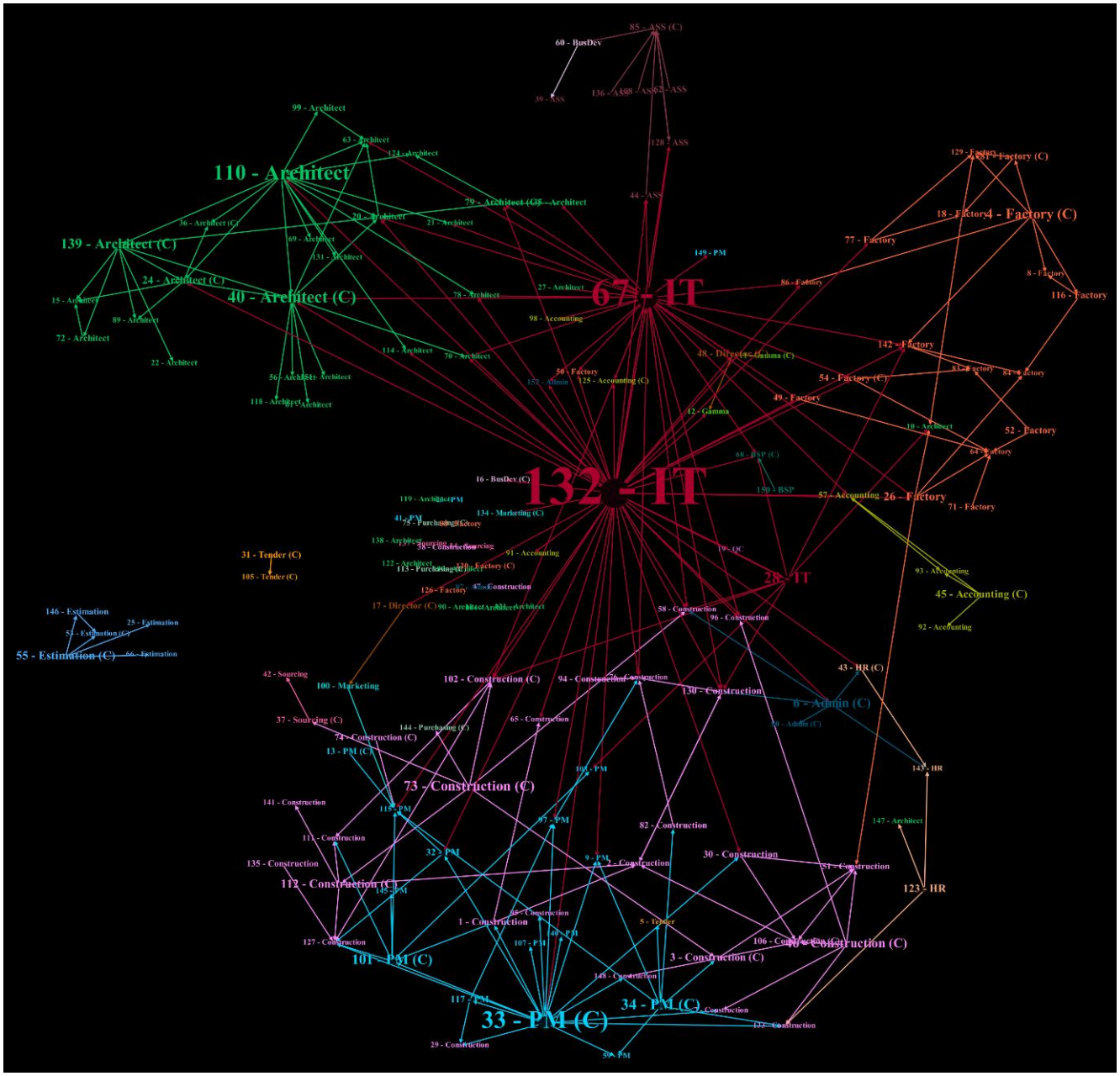


Figure 8.7. InfoSec Influence Network after the Change Program

8.3.7 Evaluating Changes in the Structures of InfoSec-Related Networks

The project team found increases of 27 per cent and 17 per cent in the densities of the InfoSec support and InfoSec influence networks respectively, and the average degrees of these two networks had increases of 27 per cent and 17 per cent. These results implied that there were more provisions of InfoSec support and exerting InfoSec influence after the change program.

The increased average degrees indicated that each employee on average had provided and received more InfoSec support and influence than before.

The out-degree centrality of the champions evaluated their abilities to directly provide InfoSec support and influence others' InfoSec behaviours. The project team observed large increases of 144 per cent and 93 per cent in the number of employees who reported to have received InfoSec support and InfoSec influence from the champions. These results indicated that the champions had successfully carried out the diffusion of InfoSec knowledge, establishing themselves as the new sources of InfoSec support and InfoSec influence as the change program had intended.

The out-degree centralisation of the networks reflected the variations in the number of outgoing ties and it determined whether the network is controlled by a few central network actors (Gesell, Barkin & Valente 2013). After the change program the InfoSec support and InfoSec influence networks respectively decreased their out-degree centralisation by 36 per cent and 30 per cent. This meant that the variations in out-degrees in these two networks had been reduced, and that there had been more employees who had high out-degrees of InfoSec support and InfoSec influence ties after the change program.

Gesell, Barkin and Valente (2013) argued that centralisation values should be below 0.25 to support a finding that actors with overly high centrality in the network had been decentralised. The centralisation values of the InfoSec support and InfoSec influence networks after the change program were 0.403 and 0.283 respectively. Although the centralisation values of these networks had been reduced, they indicated that both networks were still quite centralised based on Gesell, Barkin and Valente's (2013) threshold. While such a threshold might be desirable for other diffusion programs that aim at maximising individuals' adoption, the project team argued that InfoSec support would require some degrees of centralisation (i.e., hierarchy in the network). This was to ensure that only some employees such as the BSP or IT staff or the champions would provide other employees with InfoSec support, and it would be easier for TTT to train these employees to provide InfoSec support of consistent quality.

Reciprocity of the InfoSec support and InfoSec influence networks increased by 162 per cent and 71 per cent respectively, which indicated that employees mutually exchanged more InfoSec support and InfoSec influence after the change program. However, the reciprocity values of both networks after the change program were 0.05 and 0.016, much lower than Gesell, Barkin

and Valente's (2013) recommended threshold of 0.5. Although the InfoSec-related networks' reciprocity increased as intended, the results suggested that these networks' reciprocity would require further improvements.

Transitivity describes the tendency of nodes to form small clusters that facilitate the flow of resources in ways that all members within those small clusters can evenly receive resources (Borgatti, Everett & Johnson 2013; Hanneman & Riddle 2005). Low transitivity implies that a network has a hierarchical structure and it is often desirable to increase transitivity to achieve better circulation of resources (Gesell, Barkin & Valente 2013). The changes in transitivity of the networks were interesting. The InfoSec influence network became more transitive, with transitivity value increasing from 0.274 to 0.333, while the InfoSec support network became less transitive after the change program, with transitivity value decreasing from 0.456 to 0.335.

The increase in the InfoSec influence network's transitivity implied that employees received more InfoSec influence than before the change program. Since the SAOM analysis' results suggested that employees developed more favourable climate perceptions of their colleagues' InfoSec behaviours as they had more InfoSec influencers, such increased transitivity that facilitated the emergence of InfoSec influencers was desirable. The decrease in the InfoSec support network's transitivity indicated that the network became more hierarchical after the change program. Such a hierarchical structure was acceptable as it enabled TTT to control for the quality of the provided InfoSec support more easily if employees sought InfoSec support from a handful of providers. The decrease in transitivity also suggested that employees after the change program had changed their preference to seek InfoSec support from the official sources (i.e., the champions and the IT and BSP staff), rather than arbitrarily asking someone.

Table 8.4 summarises the changes in the InfoSec support and InfoSec influence networks. The statistics of the network features of these two networks before and after the change program are presented along with the change percentage.

Table 8.4. Network Changes Reflected by Quantitative Measures

KPI for network improvements	InfoSec support network			InfoSec influence network		
	Before	After	% change	Before	After	% change
Density (whole network)	0.014	0.017	+27%	0.009	0.011	+17%
Average degree	2.053	2.612	+27%	1.375	1.612	+17%
Out-degree centrality (champions)	59	144	+144%	54	104	+93%
Out-degree centralisation	0.626	0.403	-36%	0.404	0.283	–30%
Reciprocity	0.019	0.050	+162%	0.010	0.016	+71%
Transitivity	0.456	0.335	–26%	0.274	0.333	+21%

Within-department density in the context of this project described the connectedness of the InfoSec support and influence networks which consisted of only employees in the same departments. In other words, these measures reflected the connectedness of 19 networks which represented the provisions of InfoSec support and exerting InfoSec influence within 19 departments in TTT. An increased within-department density would indicate that employees had become more active in providing InfoSec support and exerting InfoSec influence in their department after the change program.

Table 8.5 summarises the changes in the within-department density values of 19 departments in TTT. Overall, many departments had more internal provisions of InfoSec support and exerting InfoSec influence after the change program. Only two departments had their number of internal provisions dropped (the BSP and tender departments). The increased within-department density values were part of the project team's anticipated changes, with the increases supporting the claim that the change program was successful. The small departments of accounting, administration, business development, marketing and sourcing, which all comprised fewer than 10 staff, all had their within-department densities increased. Since these increases referred to only the internal InfoSec-related socialisation between employees in the same departments and the change program involved the diffusion of local champions in each department, such increases indicated that the champions had carried out their diffusion well.

The HR department had the largest increase in their within-department density from 16.7 per cent to 100 per cent. This meant that InfoSec support was evenly transferred among all HR staff. Large departments such as architect, construction, project management and factory all

had their within-department densities increased. Even though their increases appeared as small (e.g., from 0.4 per cent to 6 per cent for project management, or from 4 per cent to 10 per cent for factory), these changes were still considerable in practice given the large sizes of these departments.

Table 8.5. Changes in Within-Department Densities

Department	Within-department density (InfoSec support)			Within-department density (InfoSec influence)		
	Before	After	Change	Before	After	Change
Accounting	0.000	0.190	Increased	0.024	0.095	Increased
After Sale Services	0.071	0.095	Increased	0.071	0.143	Increased
Administration	0.000	0.250	Increased	0.000	0.083	Increased
Architect	0.023	0.041	Increased	0.022	0.031	Increased
Business Development	0.000	0.000	Same	0.000	0.000	Same
Business Solutions Provider	0.500	0.000	Decreased	0.500	0.500	Same
Construction	0.037	0.057	Increased	0.023	0.037	Increased
Board of Directors	0.000	0.000	Same	0.000	0.000	Same
Estimation	0.050	0.300	Increased	0.150	0.250	Increased
Factory	0.038	0.098	Increased	0.036	0.055	Increased
Gamma	0.000	0.000	Same	0.000	0.000	Same
Human Resource	0.167	1.000	Increased	0.000	0.333	Increased
Information Technology	0.333	0.500	Increased	0.333	0.333	Same
Marketing	0.000	0.500	Increased	0.000	0.000	Same
Project Management	0.004	0.063	Increased	0.011	0.063	Increased
Purchasing	0.000	0.000	Same	0.000	0.000	Same
Quality Control and Assurance	0.000	0.000	Same	0.000	0.000	Same
Sourcing	0.000	0.167	Increased	0.000	0.083	Increased
Tender	0.500	0.500	Same	0.333	0.167	Decreased

Next, the project team examined the changes in the departments' out-degrees—that is, the number of employees that had received InfoSec support and InfoSec influence from these departments. These out-degrees captured the number of outgoing ties within and between departments (i.e., internal and external provisions of InfoSec support and exerting InfoSec influence). The increased out-degrees of the departments indicated that the departments had been recognised more by all employees as important sources of InfoSec support and InfoSec influence after the change program. These changes are summarised in Table 8.6.

Table 8.6. Changes in Departments' Out-Degrees

Department	Out-degree (InfoSec support)			Out-degree (InfoSec influence)		
	Before	After	Change	Before	After	Change
Accounting	0	8	Increased	1	4	Increased
After Sale Services	4	5	Increased	7	7	Increased
Administration	2	12	Increased	1	5	Increased
Architect	29	54	Increased	30	37	Increased
Business Development	1	1	Same	1	1	Same
Business Solutions Provider	7	9	Increased	1	1	Same
Construction	32	50	Increased	22	33	Increased
Board of Directors	1	0	Decreased	1	3	Increased
Estimation	2	10	Increased	3	5	Increased
Factory	16	42	Increased	16	26	Increased
Gamma	2	1	Decreased	0	0	Same
Human Resource	2	8	Increased	1	4	Increased
Information Technology	193	138	Decreased	108	81	Decreased
Marketing	2	3	Increased	1	1	Same
Project Management	13	48	Increased	14	35	Increased
Purchasing	2	1	Decreased	0	0	Same
Quality Control and Assurance	0	0	Same	0	0	Same
Sourcing	0	2	Increased	0	1	Increased
Tender	4	5	Increased	2	1	Decreased

After the change program, many departments increased their out-degrees in both the InfoSec support and InfoSec influence networks. Among these departments, the departments of administration, architect, construction, factory and project management had large increases (i.e., 10–26 ties) in their outgoing InfoSec support ties. In other words, these departments could provide from 10 to 26 more employees with InfoSec support after the change program. The departments had also increased their exerted InfoSec influence ties albeit at smaller amounts (i.e., 2–11 ties), except the project management department which increased InfoSec influence out-degrees from 14 to 35 ties.

One of the change program's objectives aimed at decentralising the overly influential IT and BSP staff. The out-degrees of the BSP department had a slight increase while their number of outgoing InfoSec influence ties remained the same. The IT department had the largest decreases in their out-degrees in both InfoSec support and InfoSec influence networks. There were 55 and 27 fewer employees than before the change program who reported to have received

InfoSec support and InfoSec influence respectively from the IT department after the change program. These large decreases in the IT department's out-degrees indicated that the change program's objective to decentralise the influential IT staff had been achieved.

Table 8.7 summarises the evaluation of the changes in the InfoSec-related networks. Overall, all established KPIs achieved satisfactory results which indicated that the networks of InfoSec support and InfoSec influence had been improved after the change program. There were 12 departments that increased their within-department densities while 14 departments increased their out-degrees in the InfoSec-related networks. This meant that employees at TTT received more InfoSec support and InfoSec influence from other employees who worked outside of their departments than those who worked in the same departments. As such, there were more opportunities for employees to learn new InfoSec-related knowledge.

Table 8.7. Summary of the Evaluation of Changes in the InfoSec-Related Networks

KPI	Outcome	Note
Increased overall density	Satisfactory	-
Increased within-department density	Satisfactory	12 out of 19 departments had their within-department density in InfoSec support and/or InfoSec influence networks increased.
Increased average degrees	Satisfactory	-
Increased out-degrees (champions)	Satisfactory	-
Increased out-degrees (department)	Satisfactory	14 out of 19 departments had their out-degrees in InfoSec support and/or InfoSec influence networks increased.
Decreased out-degree (IT and BSP departments)	Satisfactory	-
Decreased out-degree centralisation	Satisfactory	-
Increased reciprocity	Satisfactory	-
Increased transitivity	Satisfactory	InfoSec influence network increased transitivity, whereas InfoSec support network decreased transitivity. Such a decrease was acceptable as it enabled better quality control over the provisions of InfoSec support.

8.4 Evaluation

The change program was decided to follow the train the trainers approach to improve the InfoSec environment at TTT, which comprised employees' perceptions of InfoSec climate, the provisions of InfoSec support and InfoSec influence among employees. The evaluation in this stage found that employees had provided each other with more InfoSec support and exerted

more InfoSec influence. The SAOM results indicated that the more InfoSec influencers employees had, the more likely they would develop favourable climate perceptions together. As the evaluation informed that there were more InfoSec influencers after the change program, the InfoSec climate at TTT would subsequently improve over time as well. These findings were explained to and acknowledged by top management as practical improvements of the InfoSec environment.

8.5 Reflection

8.5.1 Reflection on the Champions' Diffusion of InfoSec Knowledge

At the beginning of the stage the project team had expected that the InfoSec-related networks would be improved after the champions' diffusion of InfoSec knowledge. Our expectation and confidence were based on our selection of the champions using evidence-based criteria derived from the SNA in the action planning stage (see Chapter 6), and the champions had been trained and agreed with us on the appropriate diffusion methods in the action taking stage (see Chapter 7). However, as we did not monitor the champions' diffusion, so that the champions would not feel pressured and the change program's outcome would reflect the unbiased improvements in the InfoSec-related networks, we prepared to perform another iteration if the diffusion did not result in any improvements.

Since the improvements in the InfoSec-related networks were realised at the end of this stage, top management agreed to conclude the project without any further actions. Had the project continued further, it would be beneficial to conduct in-depth interviews with the 50 champions to learn more about their experiences during the diffusion. It would be useful to learn about any issues during the champions' diffusion and the solutions implemented. Such knowledge would be valuable for designing future training programs that aim at better preparing the champions for their diffusion of InfoSec knowledge.

8.5.2 Reflection on the KPIs for Measuring Network Improvements

The project team established KPIs for the change program that focused on increasing the number of network ties (which would indicate the increased provisions of InfoSec support and exerting InfoSec influence). However, we believed that increasing the number of InfoSec-related network ties should not be the only goal for TTT or other organisations. First, changes in the InfoSec-related networks should be based on practical needs and aligned with the

organisation's strategic objectives. In this project, our change program's KPIs were decided based on TTT's specific needs to have the champions emerge as new sources of InfoSec support and influence, and to decentralise the overly influential IT and BSP staff. Such increases might not always be desirable as there would be potential issues when any employees could provide each other with InfoSec advice and troubleshooting support. For example, some of the provided InfoSec advice and troubleshooting support might be erroneous and cause more InfoSec risks in the workplace.

Second, the KPIs for measuring improvements in the InfoSec-related networks need further refinements, especially to improve the KPIs' generalisability. More empirical research is needed to develop a set of network measures that are meaningful in the wider InfoSec context and to decide the recommended thresholds for these measures. For example, if density is considered as one of the meaningful KPI that reflects an improved InfoSec-related network, then it needs to be specified how much a density's value should be and at which values should the practitioners or researchers increase or decrease the network's density.

Table 8.7 reported that not all 19 departments at TTT had increased their within-department density values and out-degrees after the change program. If the project's time frame could be extended it would be helpful to investigate the reasons why some departments failed to increase these network measures. While there might not be any substantial reasons (e.g., these departments simply did not have the opportunities to provide more InfoSec support or exert more InfoSec influence during the four-month period), further investigations might reveal the challenges that impeded these departments' contributions to the change program and suggested opportunities for future improvements.

Quantitative measures are useful for evaluating interventions in CAR projects (Davison, Martinsons & Ou 2012). The adoption of the SNA methods in this CAR project was effective as I could quantitatively evaluate the InfoSec-related networks and present the numerical evidence of the improvements to top management. However, I noted that the evaluation only indicated the improved InfoSec-related networks at TTT and not the company's improved InfoSec that potentially resulted from these networks' improvements (such as reducing violations of InfoSec policies or mitigating InfoSec risks). It would be useful to investigate the relationship between the improved InfoSec-related networks and improved InfoSec.

8.5.3 Reflection on the SAOM Process

When I performed SAOM to analyse the social influence effects, the weighted total contagion and weight total assimilation models had some issues in the unusually large standard errors and model's non-convergence, which required the use of the score test to examine the social influence effects as recommended by Ripley et al. (2017). While it was unclear what caused such issues, I suspected the instability of the InfoSec influence network, reflected by the Jaccard index below the recommended threshold of 0.3 (Ripley et al. 2017), to be responsible. The change program may also have caused drastic changes in the InfoSec influence network and made it difficult for the SAOM analysis to detect the network's changing patterns.

The SAOM issues, which may have resulted from the network instability, were inevitable in this project as the project team purposely implemented rapid changes to improve the InfoSec workplace. We could have collected data about the InfoSec influence network at multiple points in time during the four-month diffusion by the champions. This approach would improve the stability of the InfoSec influence network by creating a series of snapshots that showed a slower transition of the network from an initial stage, where the champions had not been recognised by other employees, to when most of them had emerged as prominent sources of InfoSec influence. However, I considered this approach as impractical because repeatedly responding to the same surveys would be an exhaustive task for employees and lead to a low response rate.

8.5.4 Reflection on the Formation of InfoSec Climate

The SAOM findings supported the theoretical model about the formation of InfoSec climate (Ashforth 1985) and produced new insights into such process. The results confirmed the impact of social influence on employees' climate perceptions of colleagues' InfoSec behaviours, but not on climate perceptions of direct supervisors' InfoSec behaviours. The impact of social influence on InfoSec climate formation was found to be conditional on employees' total number of InfoSec influencers in the same department. The results also found a tendency for both types of climate perceptions to self-regulate and reach a consensus with the workplace norms, rather than developing polarised perceptions.

The InfoSec climate at TTT was formed concurrently with the champions' diffusion of InfoSec knowledge. As such, the champions would have accelerated the formation of the InfoSec climate by increasing the number of InfoSec influencers. If this project could be extended I

would perform another SAOM analysis on the InfoSec influence network and employees' InfoSec climate perceptions after the evaluation and reflection stage. This SAOM analysis would allow me to examine a more natural development of InfoSec climate without any interventions.

8.6 Chapter Summary

Consistent with the scholarly objective to study the formation of an InfoSec climate and TTT's practical need to quantitatively determine whether the change program had produced the intended outcome, the project team performed two major research activities in this stage. First, we launched the second SNA survey after the four-month diffusion of InfoSec knowledge by the champions and I performed SAOM, a longitudinal SNA method, to identify the factors and mechanisms that contributed to the formation of InfoSec climate. Second, we determined the quantitative KPIs for evaluating the changes in the networks of InfoSec support and InfoSec influence after the change program. We then examined the quantitative changes in the networks and explained the findings to top management.

The SAOM analysis confirmed the focal theory and produced additional insights into the formation of InfoSec climate at TTT (as discussed in Sections 8.3 and 8.5). The evaluation of the structural changes in the InfoSec-related networks, based on the KPIs, provided quantitative evidence supporting that the networks had improved after the change program. Key improvements in the networks included the champions successfully emerging as new sources of InfoSec support and InfoSec influence, increased provisions of InfoSec support and exerting InfoSec influence and the decentralisation of the IT and BSP staff. The top management acknowledged these improvements and agreed to conclude the project. A summary of this stage's research actions is shown in Figure 8.8.

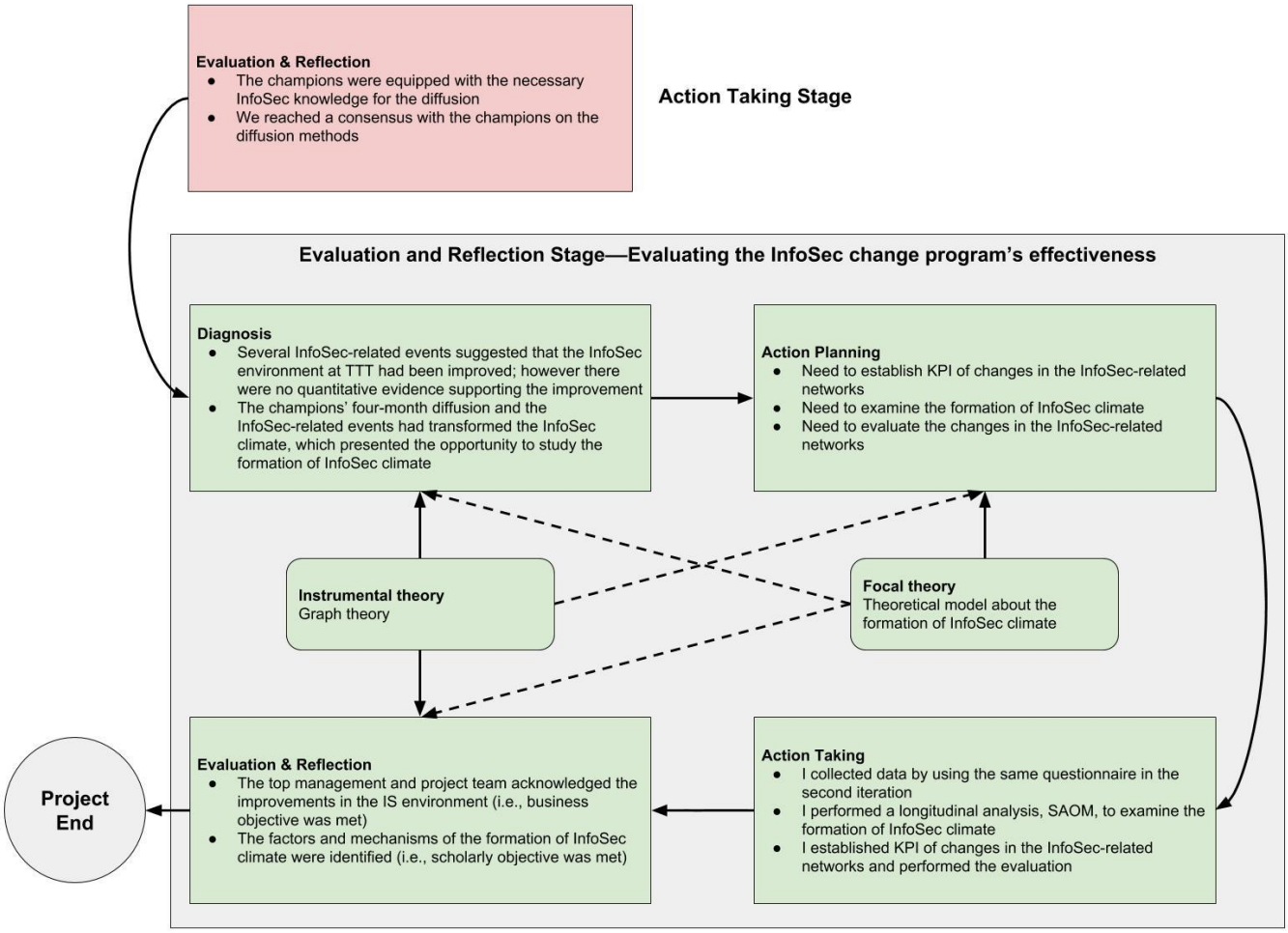


Figure 8.8. Summary of the Evaluation and Reflection Stage

Chapter 9: Discussion and Conclusion

This chapter revisits the research questions and discusses the contributions of the CAR project in three aspects—organisational, theoretical and methodological. It proposes future research directions for each of these aspects and concludes by discussing the research limitations and final considerations of this thesis.

9.1 First Research Question

My first research question aimed at identifying the factors and mechanisms which contribute to the formation of an InfoSec climate, asking:

> ***RQ1:*** *What are the factors and mechanisms that contribute to the formation of an InfoSec climate?*

To answer this research question, I reviewed the relevant literature about the forming process of an InfoSec climate and organisational climates in general (Ashforth 1985; Chan, Woon & Kankanhalli 2005; Schneider & Reichers 1983) and conducted a longitudinal SNA through SAOM (Steglich, Snijders & Pearson 2010) to examine the theoretical propositions about the formation of an InfoSec climate. In this research, InfoSec climate was represented by employees' perceptions of their colleagues' and direct supervisors' InfoSec behaviours (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013).

The forming mechanisms of an InfoSec climate included employees' socialisation with each other, which facilitated the InfoSec influence that subsequently led to the development of favourable InfoSec climate perceptions. Employees tended to receive InfoSec influence from colleagues who socialised with them, especially those who provided them with work advice, organisational updates, personal advice, InfoSec advice and InfoSec troubleshooting support and those whose job expertise they trusted. Department membership and champion status were the factors which indirectly contributed to the formation of InfoSec climate by increasing InfoSec influence between employees. Specifically, employees who worked in the same department were more likely to exert InfoSec influence over each other, and champions were more likely to exert InfoSec influence compared to non-champions.

I found that employees developed favourable climate perceptions of colleagues' InfoSec behaviours when they received influence from many InfoSec influencers in the same

departments, whose climate perceptions of colleagues' InfoSec behaviours were favourable. This finding suggested that the number of InfoSec influencers impacted the social influence's effect on the formation of climate perceptions. Moreover, climate perceptions of colleagues' InfoSec behaviours increased over time if the initial perceptions were less favourable.

In contrast, receiving influence from InfoSec influencers in the same departments did not contribute to employees' development of favourable perceptions of direct supervisors' InfoSec behaviours. Both types of climate perceptions of colleagues' and direct supervisors' InfoSec behaviours had a self-regulating tendency. Employees regulated their climate perceptions to match with those of the workplace norms, rather than developing polarising perceptions (i.e., too favourable or too unfavourable).

The SAOM analysis also identified the structural mechanisms of the InfoSec influence network, which increased the InfoSec influence that subsequently facilitated the formation of employees' climate perceptions. The results indicated that the likelihood for an employee to directly exert InfoSec influence over another employee increased when they indirectly exerted InfoSec influence over each other via multiple in-between influencers. Further, InfoSec influencers tended to become more influential and influenced employees tended to receive InfoSec influence from more people over time. Overall, the SAOM analysis confirmed Ashforth's (1985) theoretical propositions about employees' socialisation and social influence which contribute to the formation of organisational climates such as InfoSec climate. The SAOM analysis extended theoretical knowledge about the formation of InfoSec climate by revealing the contributing effects of employees' department membership and champion status, the InfoSec influence network's structural mechanisms and the changing tendencies of InfoSec climate perceptions.

9.2 Second Research Question

By reviewing the behavioural InfoSec literature and applying the problematising technique to generate research questions (Alvesson & Sandberg 2011; Sandberg & Alvesson 2010), I found that prior studies had focused on employees' individual InfoSec-related attributes and overlooked the interactions and relationships between them (see Chapter 2). Consequently, I employed SNA methods throughout this project, emphasising the analysis of interactions and relationships between individuals to investigate the formation of an InfoSec climate and to improve the InfoSec environment at TTT. This enabled me to explore the applications of SNA

methods for improving organisational InfoSec and subsequently answer the second research question:

RQ2: *How can SNA methods be used for improving organisational InfoSec?*

I employed the SNA methods in the diagnosis stage to analyse the InfoSec threats and vulnerabilities at TTT. Specifically, I visualised the InfoSec risk network based on the risk assessment's results to identify the most prominent threats and vulnerabilities based on their degree centrality. The visualisation of the InfoSec risk network and the quantitative centrality measures enabled the project team and top management to effectively diagnose the risk landscape at TTT. Based on the SNA of the risk network we determined the change program's objectives as focusing on mitigating the issues related to employees' inadequate InfoSec awareness.

In the action planning stage, I demonstrated the use of SNA methods to evaluate employees' network of provisions of organisational resources and the InfoSec influence network. The descriptive SNA enabled the project team to identify influential employees and the organisational subgroups based on their interactions with similar people. By analysing the visualised InfoSec-related networks, the project team and top management found the command-and-control InfoSec management model which had been governing the workplace's provisions of InfoSec support and InfoSec influence. This analysis enabled us to set clear objectives for our intervention, which decentralised the overly centralised IT and BSP staff in the InfoSec-related networks and increased the network centrality of the champions by having them diffuse InfoSec knowledge in TTT for four months.

The inferential SNA method ERGM was employed in the action planning stage to statistically determine employees' background characteristics and types of socialisation which increased their InfoSec influence. In particular, employees' seniority, department membership, tenure and their socialisation through the provisions of instrumental resources, expressive resources and InfoSec support were all confirmed to affect the occurrence of InfoSec influence between them. The ERGM analysis revealed the unique structural features of the InfoSec influence network at TTT which increased the likelihood for employees to exert InfoSec influence over each other. By analysing employees' socialisation in the network form, I calculated employees' network centrality which indicated their influence in the workplace. These descriptive and ERGM analyses resulted in a list of criteria to select the suitable InfoSec champions for the

diffusion of InfoSec knowledge. In the evaluation and reflection stage I performed SNA methods to quantitatively evaluate the changes in the InfoSec-related networks at TTT. Thus, I demonstrated that SNA methods have practical applications to support organisational management of InfoSec matters.

I also demonstrated the applications of SNA to examine theories through performing the ERGM and the SAOM analyses in the action planning and evaluation and reflection stages respectively. In particular, I used the ERGM method in the action planning stage to test propositions of the theory of social power bases (Raven 2008) which enabled me to determine the selection criteria for the champions. In the evaluation and reflection stage I performed a SAOM analysis to investigate a theoretical model which described the forming processes of InfoSec influence and of InfoSec climate perceptions over time. As such, I demonstrated that the SNA approach has inferential methods which can be used for testing hypotheses and produce scholarly knowledge.

From this research I found methodological contributions concerning the use of SNA methods to support CAR projects. Specifically, action researchers benefit from using the quantitative network measures to diagnose the problematic situations and to design and evaluate interventions. In fact, Davison, Martinsons and Ou (2012) emphasised the use of quantitative measures to assess the effectiveness of change programs. Action researchers performing SNA have access to a toolbox of network-based interventions, such as the intervention implemented in this CAR project which used opinion leaders to diffuse InfoSec knowledge. Action researchers employing SNA methods have many opportunities to generate novel scholarly knowledge, especially in the current context where the network research approach has not been widely considered in both the information systems and the InfoSec fields. In the following sections I discuss the research contributions of this CAR project, which were categorised into organisational, theoretical and methodological (Checkland & Holwell 1998).

9.3 Organisational Contributions

The business objective of TTT was to improve their InfoSec environment through stimulating employees' InfoSec-related socialisation which would give rise to a positive InfoSec climate. The sections below discuss the practical applications of the applied SNA methods in three areas—conducting risk assessments, selecting InfoSec champions and improving InfoSec

environments with network-based interventions and network measures, thereby answering the the second research question.

9.3.1 Social Network Analysis for InfoSec Risk Assessments

The assessment of InfoSec risks is considered as vital for organisational information systems (Loch, Carr & Warkentin 1992; Loch & Carr 1991). In addition to serving as a systematic and auditable method to identify and mitigate the InfoSec risks (Ashenden 2008; ISO 2017; NIST 2011; von Solms & von Solms 2004), recent studies found that InfoSec risk assessments which involve employees and end-users increase their acceptance of the InfoSec measures to be implemented (Spears & Barki 2010).

The involvement of TTT's department managers in the diagnosis stage's risk assessment facilitated their subsequent collaboration in the action taking stage, when these department managers were appointed as champions to perform the diffusion of InfoSec knowledge. They recalled the InfoSec threats and vulnerabilities identified in the risk assessment and, consequently, contributed their insights concerning these issues during the training workshops with other champions. They also actively engaged with top management and the project team after the workshops to further discuss the InfoSec threats in their departments and their proposed solutions. Thus, an organisational improvement that TTT achieved through performing the risk assessment was the transformation of these department managers from having little or no awareness of the company's InfoSec risks to highly aware employees. These department managers can also help colleagues in their departments comply with InfoSec requirements in the future. Further, all departments in TTT now possessed the documented procedures and materials to conduct InfoSec risk assessments.

The use of SNA methods offers an effective way to analyse InfoSec risks as a network of threats, vulnerabilities and departments. In addition to common attributes of an InfoSec risk such as likelihood, severity and cost (Bojanc & Jerman-Blažič 2008; Dhillon & Backhouse 2001; Gerber & von Solms 2005), analysing these risks and their relationships as a network provides various centrality measures to evaluate other facets of InfoSec risks. A recent study by Fuerstenau and Rothe (2014) applied SNA methods to analyse the information flow between unauthorised 'shadow' IT systems, which were considered a threat to organisational InfoSec (Furstenau et al. 2016; Silic & Back 2014b; Walters 2013). With this exception, my literature

review found that SNA methods had not been empirically applied to study organisational InfoSec risks.

As shown in the diagnosis stage, risk analysts can learn about a department's vulnerability by calculating the degree centrality of the node representing a department, which reflects the number of vulnerability nodes being tied to a department node. In this case, high degree centrality values imply that a department contains many vulnerabilities and is exposed to more threats. Similarly, the nodes representing the threats and vulnerabilities are more harmful to organisational InfoSec if they have higher degree centrality values. As such, risk analysts can evaluate both the potential and immediate severity of an InfoSec threat or vulnerability, respectively indicated by their number of connections to other nodes of the same kind or the department nodes. A vulnerability tied to many departments has tremendous severity and requires urgent attention, and a vulnerability with fewer ties to the department nodes but more ties to the threat nodes is potentially problematic.

Risk analysts can effectively communicate the InfoSec risk network to business executives as it comprehensively visualises the relations between the risks and business units such as departments. Risk analysts may also explore the similarities and dissimilarities in the patterns of nodes in a risk network. I demonstrated the use of Jaccard indices to detect groups of departments that share similar threats and vulnerabilities. This analysis allows organisations to design and implement group-based interventions which target work units that share common InfoSec issues.

9.3.2 Social Network Analysis for Selecting InfoSec Champions

This CAR project provided TTT with a group of experienced and knowledgeable InfoSec champions who supported the actual and can support future diffusions of InfoSec knowledge in the workplace. The successful diffusion in this project supports the adoption of the train the trainers or opinion leadership approach to implement InfoSec-related changes in other contexts similar to TTT. Based on my network analysis we selected InfoSec champions who met the following key criteria:

- work in the same department with the influenced targets
- hold middle management positions (e.g., department manager)
- have high degree centrality and/or Beta centrality in the networks of:
    - InfoSec influence

- provisions of InfoSec advice and/or InfoSec troubleshooting
- provisions of work advice and/or organisational updates
- provisions of personal advice and/or trust

The first selection criterion, working in the same department with the influenced targets, highlighted the critical role of the homophily effect in facilitating organisational changes. Many researchers (Burns & Wholey 1993; Cho, Wang & Lee 2012; Gesell, Barkin & Valente 2013; Greenhalgh et al. 2004; Kraatz 1998; Lewis & Seibold 1998; Rogers 1995) argue that homophily or the sharing of similar values and traits (McPherson, Smith-Lovin & Cook 2001) improves the champions' promotion of changes by facilitating frequent communication between the champions and other community members.

In line with these discussions, findings from this project's action planning and evaluation and reflection stages confirmed that employees tended to exert InfoSec influence over colleagues in the same departments. The evaluation and reflection stage's examination of the network visualisations also showed that the champions gave InfoSec support to and exerted InfoSec influence over colleagues in the same departments more than across departments. The champions' diffusion to colleagues in the same departments may have been facilitated by their close physical proximity or familiarity with the subcultures of their departments (Becker & Sasse 2017; Howell & Boies 2004; Howell & Higgins 1990; Jenssen & Jørgensen 2004).

The findings from the action planning stage confirmed that employees' seniority increased their InfoSec influence, thus, it justified the second criterion for selecting InfoSec champions. This finding is consistent with prior studies' recommendation about appointing opinion leaders who hold managerial positions (Curley & Gremillion 1983; Everett 2010; Spurling 1995). I found that employees who held a director position had even higher likelihood of influencing other employees' InfoSec behaviours than that of department managers. However, the project team did not select the directors at TTT to be InfoSec champions since they would have little time to continuously provide other employees with InfoSec advice and troubleshooting support while undertaking their regular duties.

The third criterion focused on two centrality measures, the out-degree centrality and the Beta centrality, which respectively indicated the champions' direct and indirect InfoSec influence or provisions of organisational and/or InfoSec-related resources. In addition to these centrality measures, Cross et al. (2004), Valente and Pumpuang (2007) and Liu et al. (2017) suggested

recruiting champions based on their betweenness centrality which represents the abilities of transferring resources and exerting influence across organisational subgroups. Employees with brokerage roles and boundary spanning ability, who have diverse memberships in multiple internal networks and link separate organisational clusters together, also have opinion leadership (Burt, Kilduff & Tasselli 2013; Cross et al. 2004; Fleming & Waguespack 2007). However, we did not rely on these network measures to select the InfoSec champions for the following reasons.

We prioritised selecting champions based on their direct and indirect influence, so that the champions could leverage their current influential status and quickly emerge as the new sources of InfoSec support and InfoSec influence and the IT and BSP departments decentralised as intended. Our selection was also motivated by the action planning stage's descriptive analysis which indicated that the InfoSec-related networks were transitive. Thus, we capitalised on the transitive nature of the InfoSec-related networks to facilitate the provisions of InfoSec support and InfoSec influence across separate clusters through the champions' active diffusion. Had the provisions of InfoSec support and InfoSec influence at TTT been decentralised at the beginning of the CAR project and had there been separate silos of employees, we would have prioritised appointing champions based on their betweenness centrality and brokerage abilities to connect the silos. As such, our strategy to select the InfoSec champions took into consideration the structures of the InfoSec-related networks (Greenhalgh et al. 2004; Valente 2012). On this basis, I recommend organisations to critically select the suitable network measures to recruit champions in accordance with the needs and purposes of the change programs.

Degree centrality and Beta centrality as selection criteria for the champions specifically reflect the champions' influence in the three networks which describe their provisions of 1) work advice and/or organisational updates (i.e., instrumental resources), 2) personal advice and/or trust (i.e., expressive resources) and 3) InfoSec advice and/or InfoSec troubleshooting support. These findings support Ibarra and Andrews' (1993) argument that central employees in instrumental and expressive networks have their influential status recognised by other employees. Moreover, central employees in the networks of provisions of organisational resources frequently communicate with other employees and have a greater chance to diffuse innovative ideas, thus, they are suitable for the champion role (Greenhalgh et al. 2004). My recommendation to select InfoSec champions, who are central in the network of provisions of

InfoSec support, also supports Everett's (2010) suggestion that InfoSec champions need to be able to facilitate InfoSec-related discussions in the workplace. As my research brings forward the use of SNA methods to quantitatively evaluate employees' engagement with other colleagues based on their network centrality, it enables an informed selection of InfoSec champions, rather than solely validating prior studies' discussions.

In addition to the discussed selection criteria, the analysis in the action planning stage also found other background characteristics of employees which made them appear as influential to other employees. Tenure, age and gender were all confirmed to affect employees' likelihood to exert InfoSec influence, but these characteristics were not used as selection criteria for the champions due to their small effect sizes. The confirmed positive impact of tenure on InfoSec influence supports prior studies' suggested criterion for champions (Chrusciel 2008; Howell & Higgins 1990; Jenssen & Jørgensen 2004). Conversely, the confirmed effects of age and gender on InfoSec influence may have simply reflected the unique workplace of TTT which had more young employees and an unbalanced gender ratio.

Finally, the likelihood for employees to exert InfoSec influence over each other (i.e., their potential as an InfoSec champion) was affected by the InfoSec influence network's structural features such as transitivity and the accumulative nature of InfoSec influence. These structural mechanisms negated the effects of some employee background characteristics on the likelihood of exerting InfoSec influence. Therefore, organisations should take into consideration the structures and characteristics of the InfoSec-related networks (e.g., centralised or decentralised) when determining the selection criteria for InfoSec champions.

9.3.3 Social Network Analysis for Improving InfoSec Environments

The InfoSec literature has cited many benefits of increased InfoSec communication in a workplace, such as improving employees' InfoSec knowledge and compliance, contributing to the development of an InfoSec culture and reducing InfoSec-related costs in organisations (Ashenden 2008; Bulgurcu, Cavusoglu & Benbasat 2010a; Safa, von Solms & Futcher 2016; Schlienger & Teufel 2003; Siponen 2000a; Son 2011). Similarly, ensuring employees' InfoSec compliance requires providing them with sufficient access to InfoSec-related resources and support (Herath & Rao 2009a; Warkentin, Johnston & Shropshire 2011). However, communication gaps between employees and InfoSec staff persist, which leads to InfoSec risks such as the development of insecure workarounds or employees' lack of perceived personal

responsibility for InfoSec (Albrechtsen 2007; Albrechtsen & Hovden 2009; Kirlappos, Parkin & Sasse 2014).

My research informed the unexplored use of SNA techniques to improve the InfoSec support network and the InfoSec influence network which represent the InfoSec environments. Analysing these InfoSec-related networks is important since they inform about key employees who contribute to shaping the organisational InfoSec practices, as discussed in the previous section. Moreover, analysing the network of provisions of InfoSec support enables organisations to improve the InfoSec communication in their workplaces.

Previous studies have analysed the applications of SNA techniques to improve organisational knowledge transfer and develop communities of practice, but not in relation to InfoSec (Cross et al. 2006; Hatala 2006). A recommended tactic when devising network-based interventions is to check for the overly connected employees and organisational subgroups which reflect the network's level of centralisation (Cross et al. 2006; Cross, Parker & Borgatti 2002; Müller-Prothmann 2007; Nelson 1988). Understanding network centralisation is important as it suggests the suitable types of interventions which will benefit the network. For example, Valente (2012) suggests that leader identification tactics, which rely on the use of opinion leaders to diffuse information, are especially beneficial for highly centralised networks. Conversely, decentralised networks may profit more from interventions delivering changes which are tailored for segmented groups (Valente 2012).

My visual analysis of the InfoSec-related networks in the action planning stage showed that the IT and BSP staff were nominated by most employees for providing them with InfoSec-related resources. The visual analysis further revealed that the InfoSec-related networks only had two subgroups, the architect and the factory departments, in addition to the third larger subgroup which comprised employees of the headquarters. The small number of highly connected IT and BSP staff and a few subgroups clearly indicated that the InfoSec-related networks were highly centralised. Although Valente (2012) recommended the opinion leadership approach for centralised networks to leverage the influence of highly connected people, our change program aimed at decentralising the overly influential IT and BSP staff and promoting non-IT champions as new sources of InfoSec support and influence.

Although having the influential IT and BSP staff take the champion role could maximise the diffusion's effectiveness, it would further increase employees' dependency on these IT and

BSP staff and the network's centralisation. This argument was in line with Pascale and Sternin's (2005) caution that champions may create unconstructive dependency in a workplace and discourage other employees from taking ownership over the changes. Top management and the project team agreed that appointing champions who were not overly influential at the beginning and helping them emerge as new sources of InfoSec support and InfoSec influence offer greater benefits in the long run. For example, these champions can give fast and personalised InfoSec support to their colleagues in the same department. They can also further contribute to the long-term transformation of the departments into InfoSec-aware communities where department members receive direct influence from the local champions to continuously improve their InfoSec practices.

The visual analysis of the InfoSec-related networks also revealed that TTT had been adopting the command-and-control InfoSec management model where InfoSec-related resources were controlled and distributed to all employees by a handful of IT and BSP staff. We deemed this model, which emphasised rule-following InfoSec behaviours (Son 2011) and discouraged end-users' involvement (Ashenden 2008; Kirlappos, Beautement & Sasse 2013), as unsuitable for the work culture at TTT which favoured mutual understanding and interpersonal influence between staff. Moreover, this model had the disadvantages of the IT and BSP staff potentially being overloaded with providing InfoSec support, and the potential loss of these overly influential staff causing large impacts on the company's InfoSec communication chain. Prior studies discussed that horizontal networks are effective for diffusing social influence and facilitating the development of shared meaning, whereas vertical networks are desirable for transmitting codified information and authoritative decisions (Greenhalgh et al. 2004; Rogers 1995). As such, our network-based intervention aimed at and succeeded in transforming the vertical InfoSec-related networks at TTT into horizontal ones, which was also in line with the intention to develop a shared favourable InfoSec climate.

The command-and-control structure of the InfoSec-related networks, which describes the original state of InfoSec communication at TTT before the interventions took place, deserves further discussion. Prior studies repeatedly mentioned the issues of insufficient InfoSec communication and uncontrolled employees' development of insecure practices or inaccurate understanding about InfoSec (see e.g., Albrechtsen & Hovden 2009; Ashenden 2008; Kirlappos, Beautement & Sasse 2013). The initial command-and-control structure at TTT indicated that employees identified the technical staff as reliable sources of InfoSec support

and InfoSec influence by default. As such, my research agrees with Adams and Sasse's (1999) statement that end-users should not be seen as enemies of InfoSec. In fact, they may be eager to cooperate with top management to improve company InfoSec if they receive the relevant resources via suitable communication channels. Based on the results of my study, I suggest organisations employ push tactics to proactively reach out to employees and communicate InfoSec matters to them. Network-based interventions, such as the opinion leader approach implemented in this research, effectively serve as push tactics to improve the InfoSec environment. Overall, I propose that organisations should devise network-based interventions to improve InfoSec communication by performing SNA, while flexibly aligning the interventions with their strategic objectives and current structures of the InfoSec-related networks.

9.3.4 Network Measures as New Metrics for Evaluating InfoSec Environments

Through evaluating the InfoSec-related networks in the action planning and evaluation and reflection stages, I examined the use of network measures, such as density, reciprocity and transitivity, as new metrics to assess the InfoSec environment. Current InfoSec frameworks commonly provide metrics about end-users' InfoSec which only reflect their individualistic characteristics such as InfoSec awareness, perceived accountability, numbers of possessed devices, level of access to information systems and training hours (e.g., Chew et al. 2008; Huang, Lee & Kao 2006; Kraemer, Carayon & Clem 2009; Ma, Johnston & Pearson 2008; Patriciu, Priescu & Nicolaescu 2006; Torres et al. 2006). The network measures examined in my research inform organisations about employees' and end-users' InfoSec behaviours beyond the individual level. As a result, practitioners and researchers analysing InfoSec-related network measures can quantitatively evaluate collective InfoSec performance at the work group and/or organisation levels.

Prior studies recommend several important network measures for designing and evaluating network-based interventions, which include density, centralisation, reciprocity and transitivity (Hatala 2006; Hatala & Fleming 2007; Müller-Prothmann 2007; Parise 2007; Valente et al. 2015). Gesell, Barkin and Valente (2013) recommended thresholds for these network measures which reflect a desirable state of a network after being intervened. For example, Gesell, Barkin and Valente (2013) advised that density value should be larger than 0.15, reciprocity value should be larger than 0.5 and centralisation value should be lower than 0.25 to support that the implemented interventions have successfully built connections between people.

This research used the network measures suggested by the previous studies to evaluate the InfoSec-related networks representing TTT's InfoSec environment. These measures helped the project team make informed decisions about the change program's goals such as to increase density and decrease centralisation of these networks. Although I found the implemented change program achieve the anticipated outcomes, the network measures' values after the change program were not at the recommended thresholds suggested by Gesell, Barkin and Valente (2013). However, some of these recommended thresholds may not be applicable in the InfoSec context. For example, achieving high density values for a network of provisions of InfoSec support might be undesirable in practice as it could lead to the dissemination of unofficial and erroneous InfoSec support among employees. In such a situation, organisations would need to ensure that there are governance mechanisms and standards in place to control for the quality of the disseminated InfoSec support. Consequently, the InfoSec governance must be sufficiently matured to support the utilisation of such densely connected InfoSec-related networks.

9.3.5 Considerations for Implementing InfoSec Programs and InfoSec Training

The contributions discussed so far focus on the applications of SNA. Considerations for implementing InfoSec programs and InfoSec training are discussed below. These considerations were drawn from the case study described in the diagnosis stage which consisted of interviews with the InfoSec experts in Vietnam, and from the InfoSec training workshop designed and conducted for the champions in the action taking stage.

First, the case study's findings improved TTT's understanding of the critical factors and methods for implementing InfoSec programs in the context where TTT had never conducted any InfoSec-related initiatives before. These findings were crucial for this project as they informed the project team and top management about different approaches to implement InfoSec programs, of which the train the trainers approach was adopted and subsequently improved TTT's InfoSec environment. Thus, my development of the case study highlights the importance and benefits of action researchers serving as the resource people who brings in external resources to improve research clients' problematic situations (Baskerville & Wood-Harper 1998; Greenwood & Levin 2007; Park 1999).

As discussed in Chapter 5, the case study suggested critical factors for InfoSec implementation in the Vietnamese context such as communication about rewards, sanctions or benefits of

InfoSec, many of which were also found in prior studies. Thus, the case study's findings continue to highlight the important roles of these factors in the behavioural InfoSec field. These findings also contribute to practice by informing the experts' strategies to improve their companies' InfoSec, where InfoSec matters were not prioritised by end-users and top management. The experts' insights into the strategies for implementing InfoSec programs in Vietnam can also be considered as important for the current body of knowledge where InfoSec research in non-Western contexts is scarce (Crossler et al. 2013).

From the interviews with the experts, it was clear they were aware of end-users' encountering inconvenience when they have to comply with InfoSec policies. The experts understood the Vietnamese culture, which they discussed to be collectivistic and hierarchical, and recommended persuasive methods which rely on these cultural traits. For example, they recommended explaining to employees not only the personal benefits from complying with InfoSec policies, but also how their colleagues and the whole company will benefit from their individual compliance. The experts further argued that the announcement of employees who demonstrate proficiency at InfoSec (e.g., score highly in InfoSec awareness tests or contribute to improving the company's InfoSec) would be effective in the collectivistic Vietnamese workplace. They also cautioned about the development of sub-InfoSec cultures within each department where employees follow their direct supervisors' InfoSec practices instead of following the organisation's official InfoSec directives. Similarly, the experts reasoned that such development of sub-InfoSec cultures is facilitated by employees' common perception of a large power distance in many Vietnamese firms.

Overall, I suggest practitioners and action researchers, who conduct InfoSec programs for their companies and research projects, to take into consideration the cultural traits of the focal environments when designing the programs. Although regulations and personal accountability must be followed to ensure InfoSec compliance, persuasive techniques might be more effective for convincing employees to voluntarily comply with InfoSec policies, especially in cultures similar to the Vietnamese culture. To this end, I suggest practitioners and researchers consider the SNA approach to facilitate employees' networks of InfoSec-related socialisation and persuade employees to take up and comply with InfoSec policies.

The project team applied and evaluated the experiential learning-based InfoSec training approach proposed by Karjalainen and Siponen (2011) in the action taking stage. Karjalainen and Siponen's (2011) suggested training approach not only provides a detailed step-by-step

training procedure, but also satisfies the critical elements for effective InfoSec training which were drawn from my literature review (see Chapter 7). The project team made adjustments to the suggested procedures of Karjalainen and Siponen's (2011) training approach to align its feasibility with the limited resources of the CAR project. The recommended three-stage discussion, which begins with individual reflections then sharing in pairs and in groups of four (Karjalainen & Siponen 2011), was not possible within the allocated training period of two hours per workshop. The champions at TTT had neither been formally trained in InfoSec nor had they been required to pay attention to InfoSec issues before. As a result, it would have been challenging for them if asked to critically reflect on InfoSec matters by themselves. Further, while the recommended approach maximises its effect by educating the learners on one or two InfoSec practices at a time (Karjalainen & Siponen 2011), the InfoSec training in this CAR project covered multiple topics, including InfoSec threats, internet and email practices and file management, each of which was in itself complex and contained several concepts. To cover all of these InfoSec topics while following the recommended training steps would have required more than one workshop per group of champions. Due to the limited time frame of the project and the tight work schedules of the champions, some of which were department managers, conducting a series of training of workshops was not feasible.

With these considerations in mind, the project team decided to run the training workshops in a fashion similar to a focus group. The experience gained from this CAR project suggests that the critical elements for InfoSec training, namely critical reflection and collaborative learning, can be achieved by running the workshops in such a fashion. To assist learners unexperienced in InfoSec, the trainers will have to take the leading role at the beginning and provide some background knowledge to the learners. After that, the trainers can become facilitators and let the learners lead their group discussions, while encouraging everyone to voice their opinions and maintaining the workshop's atmosphere to be opened and relaxing. The atmosphere of this CAR project's InfoSec workshops was similar to that of the successful workshops described in the study of Albrechtsen and Hovden (2010). In line with the suggestions of the InfoSec experts interviewed in the diagnosis stage, having the project team participate in the workshops as trainers also provided the champions with rich discussions about internal and external InfoSec issues.

A critical component of the experiential learning cycle-based InfoSec training approach is the active evaluation which involves reflective exchanges between the trainers and the learners

(Karjalainen & Siponen 2011). This active evaluation involves the use of a 'learning contract' (Kirkpatrick 2006) formed from the critical reflection and collaborative learning activities (Karjalainen & Siponen 2011). In this CAR project the project team asked the champions to prepare InfoSec proposals which detailed their departments' unique InfoSec threats and proposed solutions for these threats. The champions were then asked to engage in constructive discussions with the project team to finalise the proposals. The InfoSec proposals facilitated the exchange of feedback between the project team and the champions, while allowing the champions to reflect on the taught concepts and apply them to analyse their local InfoSec environments. Moreover, the project team also understood more about the champions' InfoSec environments.

Although the project team withdrew to the training sessions' background after providing InfoSec knowledge to the champions and encouraged them to lead the discussions, this approach may have restricted the champions' exchanges of ideas and experiences. Another disadvantage of this approach is that the focus group discussions may be less effective in terms of facilitating the champions' process of co-discovering knowledge, compared to the 'Think-Pair-Share' procedure recommended by Karjalainen and Siponen (2011). The InfoSec proposals containing the departments' InfoSec issues and solutions, which were prepared by the newly trained champions, might be inaccurate due to the champions' inexperience. Nevertheless, we decided that these adjustments to Karjalainen and Siponen's (2011) training approach were necessary for this project where the champions lacked InfoSec knowledge and the training's time was limited. Having the champions prepared the InfoSec proposals provided them with an opportunity to critically reflect on and apply the learned knowledge in practice.

Similar to the development of the case study in the diagnosis stage, the research actions which involved adjusting and conducting Karjalainen and Siponen's (2011) training approach aimed to prepare for the major intervention of this CAR project, the diffusion of InfoSec knowledge through champions. Thus, a full evaluation of the adjusted experiential learning cycle-based InfoSec training, including the champions' experience during the training, was not the emphasis of the CAR project. My observation and informal discussions with the champions during the training period suggested that they enjoyed learning about InfoSec matters by participating in the training activities. Further, the InfoSec training performed in the action taking stage benefitted TTT by contributing the training procedure and materials useable for

future training workshops. Table 9.1 summarises the discussed organisational contributions and their recommendations.

Table 9.1. Summary of Organisational Contributions and Recommendations

Organisational Contributions	Recommendations
• Demonstration of the use of SNA methods for InfoSec risk assessment	• Risk analysts can perform SNA to assess InfoSec risks by: o Identifying critical InfoSec vulnerabilities and threats based on network centrality o Identifying departments which shared similar InfoSec vulnerabilities and threats o Determining which InfoSec vulnerabilities and threats are commonly related to each other o Determining the common 'root' InfoSec vulnerabilities and threats
• Demonstration of the applications of SNA for improving InfoSec environment • Recommendation of the selection criteria for InfoSec champions	• Organisations can perform SNA to: o Examine opportunities for interventions through analysing visualisations and InfoSec-related network measures o Design network-based interventions and select suitable ones from prior studies o Evaluate interventions based on network measures o Identify influential InfoSec champions
• Critical factors and methods for InfoSec implementation in Vietnam as a non-Western context • Suggestion of a customised version of the experiential learning cycle-based InfoSec training approach for small groups of employees	• InfoSec practitioners are advised to: o Take into consideration the cultural traits of the work environments when designing InfoSec programs o Consider using the customised experiential learning cycle-based InfoSec training approach for training small groups of employees • Persuasive approach to influence the employees' InfoSec behaviours might be more effective in cultures similar to the Vietnamese culture

9.4 Theoretical Contributions

Throughout the CAR stages I employed multiple focal and instrumental theories to establish the theoretical backgrounds for two major research activities, determining the influential characteristics as selection criteria for InfoSec champions and examining the mechanisms and factors that contributed to the formation of InfoSec climate. The following sections discuss the theoretical contributions of these two research activities.

9.4.1 Exploring the Determinants of InfoSec Influence

Prior studies have recommended the use of champions for implementing InfoSec improvements (Baskerville & Siponen 2002; Furnell & Rajendran 2012; Gabriel & Furnell 2011; Posey et al. 2014). However, my review of the behavioural InfoSec literature showed that there has been little research on how to select InfoSec champions. To address this knowledge gap, I adopted the theory of social power bases (Raven 2008) and opinion leadership theory (Liu et al. 2017; Valente & Davis 1999) to determine the influential characteristics of InfoSec champions.

The theory of social power bases posits that an individual can appear as influential to other people by demonstrating several types of social powers (Raven 2008), of which this research examined the informational, expert and referent powers. I conceptualised employees' projection of these social powers as their provisions of work advice and/or organisational updates, personal advice and/or trust and InfoSec advice and/or InfoSec troubleshooting support. I analysed these provisions in the form of network ties. Results from the ERGM analysis in the action planning stage and the SAOM analysis in the evaluation and reflection stage both agreed that these provisions had significant impacts on exerting InfoSec influence. As such, my research findings support the theory of social power bases' propositions about these social powers' effects on social influence.

The theory of social power bases also posits that individuals can be recognised as influential if they possess the social power to reward and/or punish other people (Raven 2008). This social power was not examined in this CAR project as there were no formal policies that established rewards and punishments for InfoSec behaviours in TTT at the time. I considered this power highly relevant to the behavioural InfoSec domain as prior studies have examined the effects of rewards and sanctions on both desirable and undesirable InfoSec behaviours (Cheng et al.

2013; D'Arcy & Devaraj 2012; Guo et al. 2011; Herath & Rao 2009b; Hovav & D'Arcy 2012; Siponen, Mahmood & Pahnila 2014; Sommestad et al. 2014; Vance, Siponen & Pahnila 2012). However, these studies focused on the nature of rewards and sanctions as organisational practices rather than on the organisational members that carry out rewards and sanctions. Future studies on employees' abilities to reward and sanction from a network perspective would complement the existing knowledge. Researchers could identify characteristics of employees who were nominated by peers as capable of rewarding or sanctioning InfoSec behaviours. Similar to this CAR project's results concerning InfoSec influence, these nominated employees may not necessarily hold formal authoritative power and still be influential. It would also be interesting to explore the structural features, that is, reciprocity and transitivity of the networks of rewarding and sanctioning InfoSec behaviours.

Next, I followed opinion leadership theory (Liu et al. 2017; Valente & Davis 1999) to select InfoSec champions based on their network centrality. While I did not perform any tests to statistically determine the impacts of the champions' network centrality on their InfoSec influence, results from the evaluation and reflection stage's evaluation indicated that these champions had emerged as influential sources in the InfoSec influence network. This finding extends opinion leadership theory by suggesting that Beta centrality might effectively serve as a centrality measure for selecting influential opinion leaders in addition to the other recommended measures of degree centrality, betweenness centrality and closeness centrality (Liu et al. 2017). Future behavioural InfoSec studies are encouraged to perform SNA to statistically evaluate the effectiveness of different centrality measures on employees' abilities to provide InfoSec support or to exert InfoSec influence. Acquiring knowledge about the impacts of employees' centrality on these abilities might enable a more accurate selection of InfoSec champions.

9.4.2 Mechanisms and Factors of InfoSec Climate Formation

Through SAOM analysis I empirically examined the theoretical model which explained the formation of InfoSec climate (Ashforth 1985; Schneider & Reichers 1983). According to this model, the social influence among employees, which is facilitated by their socialisation, shapes their shared perceptions of organisational climate (Ashforth 1985; Schneider & Reichers 1983). In this CAR project, the examined InfoSec climate comprised employees' perceptions of their colleagues' and direct supervisors' InfoSec behaviours (Chan, Woon & Kankanhalli 2005; Goo, Yim & Kim 2014; Jaafar & Ajis 2013).

There is little research that has explored the formation of an InfoSec climate, much less from a network perspective which conceptualises employees' socialisation and social influence as network ties. Jaafar and Ajis (2013) and Goo, Yim and Kim (2014) focused on the outcomes of an InfoSec climate (i.e., InfoSec commitment and compliance) rather than on its formation. Chan, Woon and Kankanhalli (2005) examined the effect of socialisation on InfoSec climate, but their conceptualisation of InfoSec climate as a one-dimensional construct was not consistent with prior research on organisational climates (Goo, Yim & Kim 2014). Further, their conceptualisation of socialisation as employees' perceptions overlooked the structural features of socialisation. Testing the effect of employees' perceived level of socialisation on InfoSec climate perceptions (Chan, Woon & Kankanhalli 2005) provides little insight into the underlying mechanisms, such as the structural features, types of socialisation or the characteristics of the influencers and of the influenced employees, which facilitate the formation of an InfoSec climate.

My SAOM findings indicated that employees' socialisation through the provisions of instrumental resources, expressive resources and InfoSec support increased the likelihood of exerting InfoSec influence which subsequently forms an InfoSec climate (see Chapter 8). These findings confirm the theoretical explanations for the formation of organisational climates by Schneider and Reichers (1983) and Ashforth (1985), which posit that organisational climates such as that about InfoSec can be shaped as a function of employees' socialisation and social influence. The findings extend such explanations by elaborating on the details of the formation process of InfoSec climate, especially that the social influence which facilitates the formation of InfoSec climate occurred only among members of the same departments, and that the impact of social influence on employees' perceptions of InfoSec climate was affected by the number of InfoSec influencers these employees were exposed to.

The SAOM analysis further contributed new theoretical insights by confirming that social influence only impacted employees' climate perceptions of colleagues' InfoSec behaviours. The climate perceptions of direct supervisors' InfoSec behaviours were unaffected by social influence. Instead, employees tended to regulate their perceptions of direct supervisors' InfoSec behaviours to become more favourable or unfavourable when their own initial perceptions were unfavourable or favourable respectively. The climate perceptions of colleagues' InfoSec behaviours also had this tendency to self-regulate. Further, I found the development of both types of climate perceptions to follow the workplace norms. Employees

favoured adjusting climate perceptions to match with the average level of the workplace and they avoided developing polarising climate perceptions. Table 9.2 summarises the theoretical contributions discussed in this section and their respective recommendations.

Table 9.2. Summary of Theoretical Contributions and Recommendations

Theoretical Contributions	Recommendations

• Examination of the theory of social power bases and opinion leadership theory in the InfoSec context by:
  ○ Identifying the non-network determinants of InfoSec influence
  ○ Suggesting the use of network centrality measure as selection criteria for InfoSec champions
	• The theory of social power bases was supported by the ERGM analysis, where the power bases were conceptualised in the form of network ties between the employees instead of their perceptions
	• The increased InfoSec influence and provision of InfoSec resources by the selected champions, and the SAOM results provided evidence supporting opinion leadership theory

• Confirmation and extension of current knowledge, which explain the formation of InfoSec climate	• The SAOM results showed that:
	  ○ InfoSec influence network was transitive; InfoSec influence accumulated over time
	  ○ InfoSec influence developed climate perceptions of colleagues' but not direct supervisors' InfoSec behaviours
	  ○ Total number of InfoSec influencers in the same departments affected climate formation
	  ○ Climate perceptions tended to self-regulate in accordance with the workplace norms

9.5 Methodological Contributions

This section discusses the methodological contributions of my research which concern the use of SNA methods in CAR projects. Additionally, I reflected on my experience of conducting this CAR project and proposed improvements to the CAR process.

9.5.1 Using Social Network Analysis Methods in Canonical Action Researches

Designing and evaluating interventions are critical activities in many AR projects as these activities provide researchers with the opportunities to improve the focal organisational situations and generate scholarly knowledge while doing so (Baskerville & Myers 2004).

Similar to my research, AR in the information systems domains have also studied diffusion by opinion leaders, but these studies' selection of opinion leaders and their evaluation of outcomes mostly relied on qualitative methods. I discuss some examples of this type of AR below.

Urquhart and Lennox (1999) studied the diffusion of information that influences farmers' IT adoption, which involved opinion leaders participating in group meetings with the farmers. The characteristics of these opinion leaders were rather unclear and the opinion leaders' contributions to the diffusion were inferred through analysing qualitative discussions. Börjesson, Martinsson and Timmerås (2006) utilised both push and pull tactics to diffuse a new work practice with the assistance of two change agents and nine opinion leaders respectively. Börjesson, Martinsson and Timmerås (2006) selected the change agents and opinion leaders based on characteristics such as technical competence and social skills and being well respected among peers. Their evaluation of the change agents and the opinion leaders' contributions to the diffusion was also based on qualitative analysis. Holmberg et al. (2009) investigated the introduction of a new software process improvement initiative in a telecom firm, which involved the participation of one of the authors who acted as a change agent. Holmberg et al. (2009) deduced from interview findings that the change agent's participation was critical for the diffusion.

I found that the numbers of opinion leaders, change agents and champions employed for the diffusion in these studies were few. Although these studies acknowledged the important roles of opinion leaders in supporting the diffusion of innovations, they put little emphasis on the selection criteria of the champions. Their selection of the leaders, which claimed to be based on the persons' influence but did not provide any measurement of such influence, may have missed important individuals who were more suitable for the opinion leader role. This argument also applies to the selection of other diffusion roles such as change agents. Consequently, action researchers may not be able to accurately study the phenomena which resulted from a diffusion facilitated by ineffective opinion leaders. To this end, action researchers may find SNA methods useful in providing the network measures, such as degree centrality and Beta centrality, to quantitatively evaluate the potential opinion leaders' social influence. Moreover, using the SNA approach enables action researchers to evaluate the potential of as many community members as they can, thus, enabling a selection of a large quantity of effective opinion leaders.

The SNA approach provides action researchers with a toolbox of numerous network-based interventions beyond enabling them to quantitatively select key people for the diffusion. For example, Valente (2012) promotes network-based interventions which involve delivering tailored changes to segmented groups. Action researchers may perform SNA to detect cohesive groups of nodes (i.e., organisational subgroups or cliques) based on their common connections (Malliaros & Vazirgiannis 2013). After identifying the groups, action researchers can deliver group-based interventions separately or sequentially (Valente 2012). Strategies for network-based interventions also focus on non-central community members such as using SNA methods to identify peripheral or isolated members and perform interventions to bring them to the larger communities or to make use of their untapped expertise and knowledge (Cross, Parker & Borgatti 2002; de Toni & Nonino 2010; Valente 2012). Action researchers may employ and study these various network-based interventions as their studies' change programs.

Action researchers may find SNA methods useful for diagnosing the focal situations before interventions. The examination of network measures such as density and centralisation, which describe the level of interactions between community members, can justify the need for performing interventions and assist action researchers in planning the interventions. These network measures also provide the quantitative evidence to evaluate the change program's outcomes, in line with Davison, Martinsons and Ou's (2012) recommendation concerning the use of quantitative measures to evaluate CAR's interventions. Using SNA methods to evaluate networks of diffusion informs action researchers about not only the level of adoption, but also the patterns of the diffusion. Information about which community members initiated or received the diffusion is valuable for measuring opinion leaders' performance and for planning the follow-up actions after an intervention. Such patterns cannot be captured by using a traditional survey which simply asks whether community members adopt the changes or not and to which level. Cross, Parker and Borgatti (2002) found that showing the network visualisations to industry partners as research collaborators was an effective way to instigate non-confrontational conversations about overly influential or isolated employees in a workplace. In this CAR project, the top management at TTT displayed great interests in examining the networks of employees' socialisation and I found it easy to discuss the networks with top management during our milestone meetings. Therefore, I argue that action researchers employing SNA methods can effectively communicate the network visualisations to their research clients, facilitating collaboration and improving mutual understanding of the organisational situations.

9.5.2 Reflection on the CAR Approach

I adopted the CAR approach for this project after comparing it with nine other approaches to AR (see Chapter 3) listed by Baskerville and Wood-Harper (1998). Only CAR, action science and clinical field work aimed at both organisational development and producing scientific knowledge and only the CAR approach enabled an iterative and collaborative research process that suited my project with TTT. Collaborative practice research (CPR) (Mathiassen 2002) is an approach to AR (Davison, Martinsons & Kock 2004) that is considered as a variation of the CAR approach (Cole et al. 2005). Mathiassen (2002) and Mathiassen and Sandberg (2013) describe CPR as an AR approach which focuses on researchers' close collaboration with practitioners through analysis to understand practice, develop new propositions and artefacts to support practice and improve practice through interventions. Researchers recognise the CPR approach's methodological pluralism as one of its distinctive features, as it emphasises the combined use of collaborative implementation, controlled experimentation and practice observations in conducting AR (Barqawi, Syed & Mathiassen 2016; Goldkuhl 2011; Mathiassen & Sandberg 2013).

To go beyond my research project and discuss the advantages and disadvantages of different AR approaches I compared the CAR approach with the CPR approach below. My comparison examines the process model of these approaches, which focuses on three steps, 1) initiating, 2) iterating and 3) closing (Iversen et al. 2004). Based on the reflection of my CAR project, I provide additional methodological contributions concerning the adoption of the CAR approach.

The CAR approach follows the iterative five-stage process model of Susman and Evered's (1978) approach (Davison, Martinsons & Kock 2004). Given that CPR projects can flexibly take different forms, I chose to analyse Iversen et al.'s (2004) research as an exemplary example of a CPR project, as it is based on Mathiassen's (2002) original description of the CPR approach and Mathiassen was also a co-author of this study. That particular CPR project adapted elements of McKay and Marshall's (2001) and Checkland's (1991) approaches to AR.

Checkland proposes an AR approach that begins with the researchers defining a research agenda through establishing the research framework (F) and methodology (M) for their research (Checkland 1991; Checkland & Holwell 1998). Then, the researchers apply these F and M elements to study the phenomena in a real-world problem situation (A) through

performing research actions and reflecting on the implemented actions (Checkland 1991; Checkland & Holwell 1998). McKay and Marshall (2001) describe their approach's process model as consisting of two overlaid research cycles which represent the researchers' problem-solving and research activities that operate in tandem with each other. McKay and Marshall's (2001) process model begins with the researchers identifying the research interests and the real-world problems, which both contribute to the formulation of an action plan, followed by the iterative actions to implement and evaluate the outcomes of such plan.

Researchers performing CAR initiate the research project by developing an RCA which outlines the project stakeholders' roles and facilitates mutual understanding about the project's essentials such as goals and key actions (Davison, Martinsons & Kock 2004). When performing their CPR project, Iversen et al. (2004) also developed a RCA which is in line with the CAR approach (Davison, Martinsons & Kock 2004; Susman & Evered 1978). The CPR approach does not put explicit emphasis on developing such an agreement, and the researchers may initiate a CPR project by establishing a collaborative space which provides information about the collaboration structure of a CPR project, including details of the stakeholder groups in the project and their methods of collaboration (Mathiassen 2002). Researchers can initiate a CPR project by identifying a real-world problem and by reviewing relevant literature to come up with an action plan (see Iversen et al. 2004). These initiating activities are consistent with those described in the AR approaches proposed by Checkland (1991) and McKay and Marshall (2001). In this aspect, the CAR approach's initiating step (Davison, Martinsons & Kock 2004; Davison, Martinsons & Ou 2012) differs from that of the CPR approach by not putting emphasis on identifying the researchers' research and problem-solving interests, and it focuses more on diagnosing the local problematic situation.

With regard to the iterating step, both the CAR and the CPR approaches emphasise the close researcher–client collaboration and the adoption of methodological pluralism throughout the iterative process (Davison, Martinsons & Kock 2004; Davison, Martinsons & Ou 2012; Mathiassen 2002). However, the two approaches have different methods to achieve the dual imperatives of AR (i.e., generating scholarly knowledge while improving the focal problematic situation) (Davison, Martinsons & Kock 2004; Goldkuhl 2012a; McKay & Marshall 2001).

To ensure the generation of scholarly knowledge while improving the problem situation, the CAR approach uses a process model where the evaluation of the intervention's outcomes and the reflection to detect research contributions are iteratively performed (Davison, Martinsons

& Kock 2004; Susman & Evered 1978). Moreover, Davison, Martinsons and Ou (2012) recommend researchers to employ instrumental theories, which include tools and models such as data model, balanced score card and selective coding technique, during the diagnosis stage. At the end of the diagnosis, the researchers identify a focal theory that provides theoretical explanations for the iteration's anticipated outcomes and guides the research actions (Davison, Martinsons & Ou 2012). The adoption of these theories helps the researchers maintain their focus on the task to produce scholarly knowledge from the CAR project. The achievement of the dual imperatives is further ensured by having the researchers conform with a list of criteria for research rigour (see Davison, Martinsons & Kock 2004) which serves as an elaborate guide for the research activities performed within each iteration. On the other hand, the CPR approach provides researchers with a more flexible process model which involves three types of activities, namely, 1) interpret collected data to understand, 2) design to support and 3) intervention to improve, which respectively produce three types of knowledge, 1) concepts and frameworks related to practice, 2) propositions and artefacts to support practice and 3) the knowledge about what it takes to implement the interventions that improve practice (Mathiassen 2002).

The CAR approach considers the diagnosis as part of a singular five-stage cycle that constitutes an iteration (Davison, Martinsons & Kock 2004; Susman & Evered 1978), where the researchers interact with organisational stakeholders to investigate the current problematic situation. Similarly, Mathiassen (2002) describes both the diagnosis of the problematic situation and studying relevant literature as part of the CPR approach's iterative three-stage cycle. While Checkland (1991) also describes an iterative process model that comprises a singular cycle in his approach, McKay and Marshall's (2001) approach has a different iterative structure which consists of two interrelated cycles. Researchers who follow McKay and Marshall's (2001) approach instigate a cycle by identifying the research interests and problems and by designing an action plan. This cycle then leads to one or more smaller iterative cycles where the action plan is revised and executed until satisfactory results can be achieved (see Figure 9.1). The diagnosis and action planning stages are in Cycle 1. At the exit point of Cycle 2, where the researchers iteratively revise and implement actions to achieve satisfactory outcomes, they may identify follow-up problems and research interests which instigates a new Cycle 1.

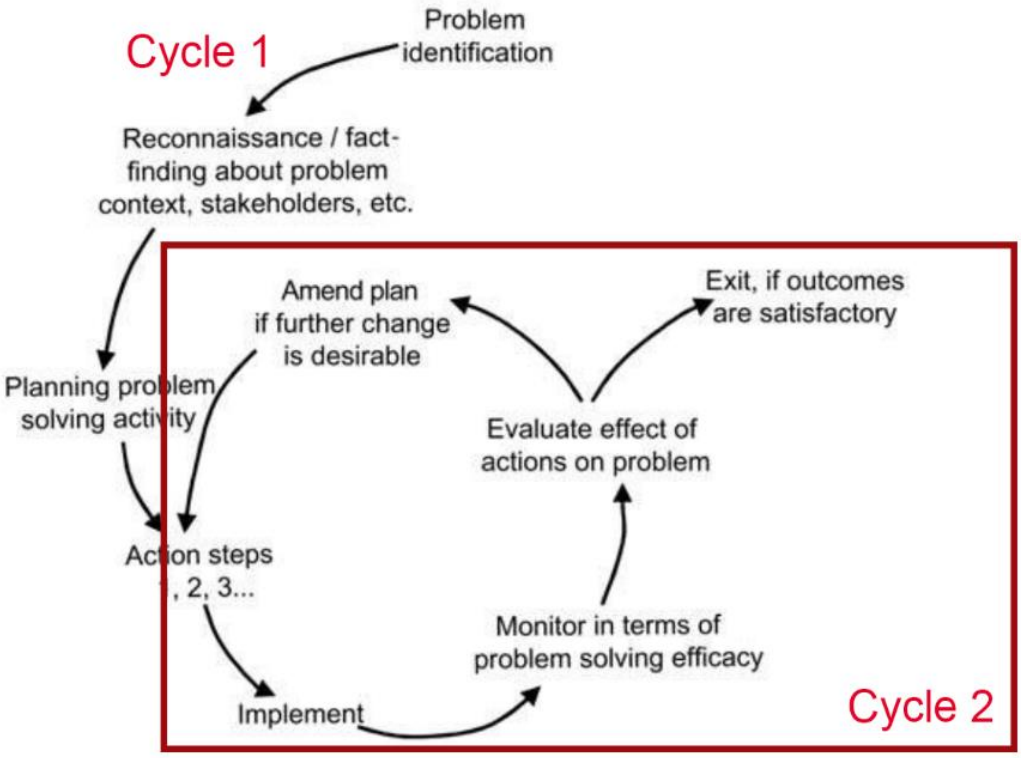


Figure 9.1. Generic Action Research Approach

Adapted from McKay and Marshall (2001).

Davison, Martinsons and Kock (2004) specified in the principle for the CPM that researchers who perform CAR need to explain the condition of their exit and the project's conclusion (i.e., the scholarly and business project objectives being met). Moreover, the researchers and the collaborating clients are suggested to jointly reflect on the decision to conclude the project at the end of each iteration (Davison, Martinsons & Kock 2004). Similarly, McKay and Marshall's (2001) process model, which Iversen et al. (2004) adapted for their CPR project, also suggested researchers to iteratively evaluate the project outcomes and decide their exit. Therefore, I consider both the CAR and the CPR approaches to have similar closing steps. Table 9.3 summarises the CAR and CPR approaches' activities in the three AR steps.

Table 9.3. Comparison between the Collaborative Action Research and the Collaborative Practice Research Approach

	CAR	CPR
Initiating	1. Establish the client–system infrastructure	1. Establish collaborative space 2. Appreciate problem situation 3. Study literature 4. Select solution
Iterating	2. Diagnosis 3. Action planning	5. Develop framework for solution 6. Design solution

	4. Action taking 5. Evaluating 6. Specifying learning	7. Apply solution 8. Evaluate experiences
Closing	7. Exit if business and scholarly objectives are achieved	9. Exit 10. Assess usefulness 11. Elicit research results

CAR component adapted from Davison, Martinsons and Kock (2004), Davison, Martinsons and Ou (2012), Susman and Evered (1978). CPR component adapted from Hansen (2009), Iversen et al. (2004) and Mathiassen (2002).

While both the CAR and CPR approaches have similar goals and activities for the initiating and closing steps, I found the iterating step of these approaches have their own advantages and disadvantages.

The CAR approach is advantageous because it emphasises the adoption of focal and instrumental theories in every iteration, which assists researchers in producing scholarly knowledge while performing the practical interventions (Davison, Martinsons & Ou 2012). Moreover, researchers performing CAR repeatedly follow a fixed process from diagnosing the current situation to reflecting on the outcomes of each iteration. This intensive research and problem-solving process enables researchers to constantly improve the problematic situation and it maximises the opportunities to generate scholarly outputs through the iterations. However, my experience of following the CAR process detects a potential issue that the researchers may lose sight of their main objectives when they follow such an intensive process. When I diagnosed the situation after the champions' diffusion of InfoSec knowledge, I found it tempting, from a researcher's perspective, to generate more theoretical knowledge by adopting additional theories to investigate the champions' process of diffusing InfoSec knowledge and employees' reactions to the diffusion. However, exploring the diffusion of InfoSec knowledge had little relevance to both the scholarly and business objectives of this CAR project, and using the limited project time frame for such purpose would be considered unproductive.

The CAR's list of 31 criteria for rigour (see Section 9.6 below), which guides the research activities to achieve the dual imperatives, might be considered as excessive. By attempting to satisfy these criteria the researchers might make the CAR project and the researcher–client collaboration become overly formal and complicated. Satisfying all of these criteria would be challenging for complex projects that involve multiple organisations and stakeholders. However, Davison, Martinsons and Kock (2004) comment that a CAR project may not necessarily adhere to all of these criteria, although they note that failing to meet any of the

criteria may raise reviewers' and editors' concerns in a publishing context. The exhaustive list of the criteria may also effectively serve as a structured guide to ensure that projects carried out by inexperienced researchers, as was the case in this project, can achieve rigour.

On the other hand, the more flexible CPR approach (see Mathiassen 2002) offers the freedom and flexibility to accommodate different levels of project complexity. Researchers who perform CPR are not required to adhere to any fixed process model (Iversen et al. 2004) and CPR projects can flexibly employ the generic AR process (McKay & Marshall 2001) to guide the research and problem-solving actions. McKay and Marshall's (2001) process model encourages the researchers to understand the real-world problem of interest and to study the literature, which enable them to establish clear objectives before entering the iterative process to work in the local context. The CPR approach is thus advantageous in this aspect. However, it might require the action researchers to be experienced to ensure research rigour since the CPR approach does not provide a detailed guide for rigour, and less experienced researchers may omit important activities that would make them unable to achieve the dual imperatives of action research.

On this basis and on my experience of this CAR project, I provide some recommendations to further improve the CAR process. Researchers might adapt the initiating activities of the generic AR process (McKay & Marshall 2001) to study practice and real-world problems and to establish research questions before committing to the CAR project. By doing so, the researchers can envision how the potential CAR project will contribute to theory and practice and they can maintain their focus on the project's objectives while engaging and research and problem-solving activities in the local situation.

I established in advance of the CAR project my research interest and questions, which aimed at investigating the formation of InfoSec climate and the applications of SNA methods for improving organisational InfoSec. My research actions, which were collaboratively performed with TTT, tackled different issues in each stage and the stages' outcomes contributed to addressing the established research questions. This approach of establishing the research interest and understanding practice in advance of the CAR project requires the action researchers to approach suitable collaborating practitioners. The researchers can acquire an understanding about the practice and real-world problems of interest by interacting with practitioners, potentially through conducting a case study. Problematisation (see Alvesson & Sandberg 2011) and gap-spotting techniques (see Sandberg & Alvesson 2010) can be useful

for identifying the unexplored research area, based on which the action researchers identify their research interests and research questions.

My second recommendation focuses on the use of theories in CAR projects. Davison, Martinsons and Ou (2012) discuss that the instrumental theories should support and complement the focal theories. In this research there was also a relationship between the different focal theories (i.e., the theoretical model about InfoSec climate formation and the theory of social power bases) and the instrumental theories (i.e., opinion leadership theory and graph theory)—all focused on the employees' socialisation. While the complementary roles of theories became evident in this CAR project, the current guide to performing CAR does not provide any criteria for selecting focal and instrumental theories. I considered and can now recommend some selection criteria for theories such as the instrumental theories' contributions to achieving the business objectives, the feasibility of applying the theories in the research context (i.e., whether the actual context has the elements prescribed in the theory to explain causes and effects) and a potential conflict between the adopted theories and the scholarly objectives.

Researchers may encounter such conflict in a situation where the adoption of a theory would effectively solve the problem, yet examining its propositions or reflecting on its applications would not produce new knowledge for the research community and beyond. I experienced this conflict in the action taking stage where I performed the training for the InfoSec champions; the actions performed in this stage were guided by the experiential learning cycle-based InfoSec training procedure (Karjalainen & Siponen 2011) and the critical elements for effective InfoSec training which were identified from the literature. The end results indicated that the training was successful in equipping the champions with InfoSec knowledge and in facilitating a mutual understanding about the diffusion tasks between these champions and the project team. The training as an intervention produced satisfactory results that contributed to achieving the CAR project's business objective, but a reflection on these results did not offer many theoretical contributions. It was also not within the CAR project's scope to theorise the training's process and outcomes. In fact, it would be reasonable to anticipate that training should improve the learners' knowledge. I felt the adoption of theories for designing and implementing the InfoSec training was mainly an attempt to closely conform with the CAR approach's process model, although Davison, Martinsons and Ou (2012) do not suggest that every CAR iteration or stage must have a focal and an instrumental theory. Action researchers

who perform CAR should be aware of similar situations and to make rational decisions that concern the adoption of theories to guide research actions and theorising. I further note that the incompatibility between focal and instrumental theories, and between these theories and the research context, may create opportunities to discover new knowledge as well.

Action researchers, especially less experienced ones, should be aware of the uncontrollable nature of AR projects and its consequences. In exchange for the opportunities to produce novel knowledge from investigating an unexplored research area, I felt anxious and under pressure to produce positive scholarly and practical results until the evaluation and reflection stage which indicated the champions' diffusion was satisfactory. While being an inexperienced researcher might have contributed to my insecurity, the limited time frame of a PhD candidature, which would not allow further iterations to rectify any potential issues after the diffusion, was another major cause for such insecurity. My anxiety increased when the champions were diffusing InfoSec knowledge, as I wanted to avoid creating biased outcomes and, thus, did not want to further intervene and check their performance or remind them about the diffusion. These were the uncontrollable factors of this CAR project that emotionally affected me as an action researcher. I could have taken contingency actions to ensure the generation of knowledge in the event where the champions' diffusion failed to produce satisfactory results, which would include analysing the reasons for such failure. However, if the diffusion failed to improve TTT's InfoSec environment, the business objective would not be achieved and thus the project's conclusion would have to be negotiated with the top management. In this regard, I had explained my intention to examine the untried SNA approach to improve InfoSec environment in the initial meeting before the CAR project commenced.

I suggest researchers assess the uncontrollable elements of their CAR projects and develop contingency plans for the unexpected during the diagnosis and action planning stages of a CAR iteration, something not currently emphasised in the introductory texts to CAR (Davison, Martinsons & Kock 2004; Davison, Martinsons & Ou 2012). I also advise researchers to develop a mutual understanding with the collaborating practitioners about the expectations and risks of the project as early as possible. In addition to establishing the CAR approach's recommended RCA, it might be beneficial for the researchers to adapt the concept of a collaborative space from the CPR approach (see e.g., Mathiassen 2002) to effectively facilitate the researcher–client collaboration in a CAR project. Figure 9.2 provides a summary of my recommendations to extend the CAR process.

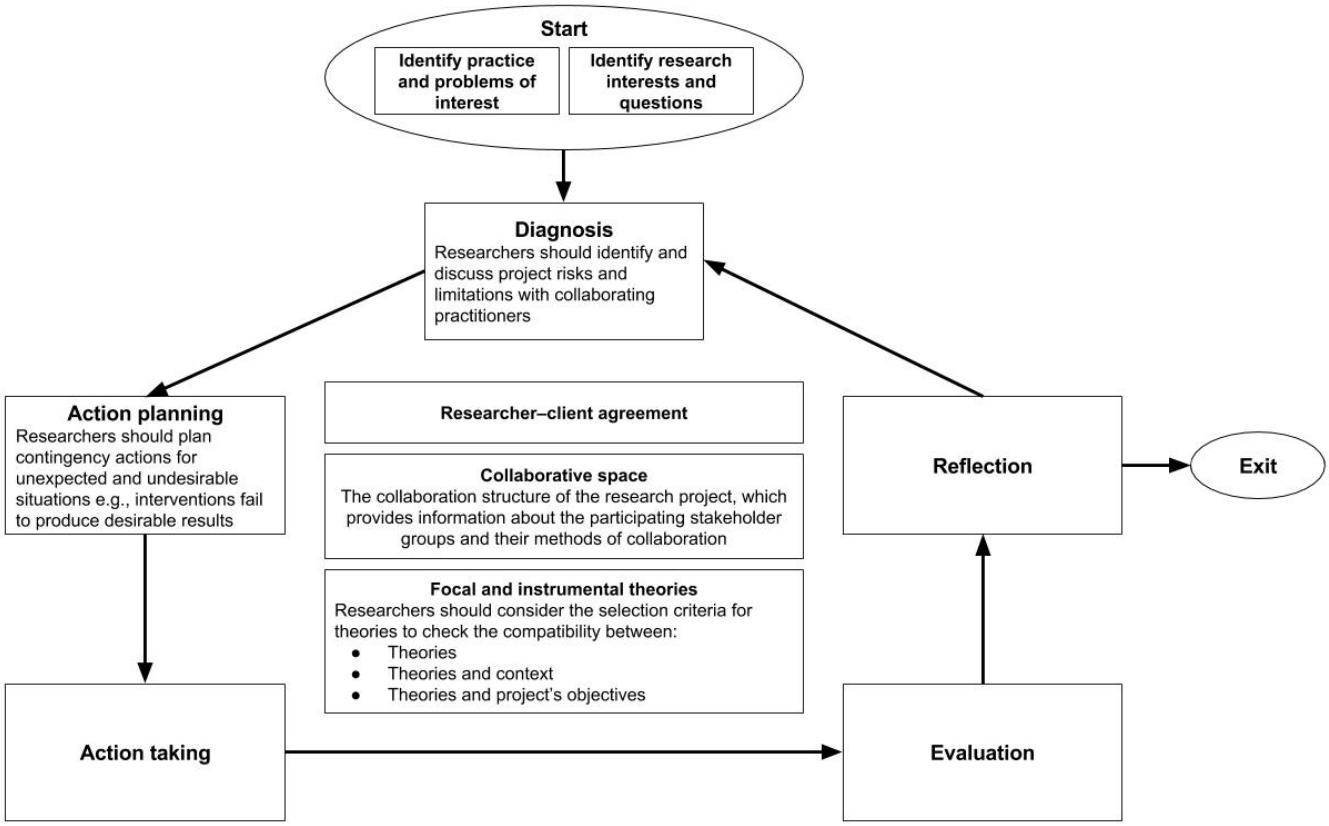


Figure 9.2. Extended Canonical Action Research Process Model

While the CPM provides a step-by-step process for conducting CAR projects consisting of five stages, namely diagnosis, action planning, action taking, evaluation and reflection (Davison, Martinsons & Ou 2012), my literature review showed that prior CAR projects had not followed any structured way to perform these individual stages. In this CAR project, I adopted the CPM to guide the research activities within each of those five stages for two reasons. First, it provided a consistent structure for describing the research process and reporting results. Second, the adoption of CPM within each stage forced me to iteratively diagnose the current situation and to plan actions that were motivated by focal and instrumental theories, which subsequently created the opportunities to perform relevant actions for the organisational context and produce theoretical contributions through continuous reflection. As an inexperienced action researcher, I appreciated the mentioned benefits of adopting the CPM to guide the activities within the CAR stages, which also helped to alleviate my anxiety when coping with the uncontrollable nature of the CAR project. Such extended use of the CPM did not conflict with the rigor of CAR described by Davison, Martinsons and Kock (2004), and it could further improve rigor and contribute to the dual imperatives of action research, i.e., achieving both business and scholarly objectives in CAR. It should be noted that this extended use of the CPM may appear to be excessive, and its benefits may be found as being outweighed by the time and efforts that

the action researchers and industry partners spend on following the CPM within each CAR stage. To this end, the development of a structured process to plan and carry out the activities within the CAR stages would be beneficial. Table 9.4 summarises the methodological contributions and recommendations of this section.

Table 9.4. Summary of Methodological Contributions and Recommendations

Methodological Contributions	Recommendations

• Demonstration of the use of SNA methods to support the CAR approach in diagnosing the organisational situation, as well as designing and evaluating network-based interventions
• Provision of recommendations to ensure the effective use of SNA methods in CAR projects
• Suggestion to improve the CAR process
	• SNA methods assist the CAR process by:
	  ○ Providing a toolbox of network-based interventions
	  ○ Providing the means to diagnose the current situations and evaluate the interventions' outcomes
	• Action researchers are advised to consider following the recommendations from the extended CAR process
	• Less experienced action researchers should be aware of the uncontrollable nature of AR projects and its consequences
	• The development of a structured process for planning and conducting activities within each CAR stage would be beneficial

9.6 Evaluating the Five Principles of CAR

As mentioned in Chapter 3, CAR projects are suggested to follow five principles to ensure their rigour—RCA, CPM, theory, change through action and learning through reflection (Davison, Martinsons & Kock 2004). This section discusses my evaluation of the overall CAR process concerning these five principles, resulting in further recommendations on conducting CAR projects.

9.6.1 Researcher–Client Agreement

The principle of RCA focuses on the establishment of mutual understanding between the action researchers and the research clients, particularly about the CAR approach and the stakeholders' duties during the projects (Davison, Martinsons & Kock 2004). Table 9.5 lists six criteria for this principle of RCA.

Table 9.5. Criteria for the Principle of Researcher–Client Agreement

1a	Did both the researcher and the client agree that CAR was the appropriate approach for the organisational situation?
1b	Was the focus of the research project specified clearly and explicitly?
1c	Did the client make an explicit commitment to the project?
1d	Were the roles and responsibilities of the researcher and client organisation members specified explicitly?
1e	Were project objectives and evaluation measures specified explicitly?
1f	Were the data collection and analysis methods specified explicitly?

Adopted from Davison, Martinsons and Kock (2004).

As described in Chapter 4, I explained the CAR approach to the top management at TTT and we agreed to perform the CAR project to achieve both scholarly and business objectives (1a and 1b). We developed and signed a written RCA which effectively served as a formal document that explicitly established the rights and responsibilities of myself as the researcher and top management as the research client. The RCA formally recognised the top management's commitment to support the data collection and to protect the respondents' anonymity (1c and 1d). My intentions to collect network data via questionnaire and to perform SNA for evaluating the project's outcome was explicitly specified in the initial meeting with TTT, which was in line with my scholarly objective to advance knowledge about the applications of SNA methods in the behavioural InfoSec field (1e and 1f).

Action researchers in the information systems domain have reported numerous benefits of establishing a formal RCA, including securing top management's support, providing researchers with the legitimacy to interact with organisational employees, reducing opportunisms and encouraging learning, and helping researchers and research clients establish mutual understanding about the project (Foorthuis & Brinkkemper 2008; Huang & Martin-Taylor 2013; Lindgren, Henfridsson & Schultze 2004; Malaurent & Avison 2016). The principle of RCA also concerns the clear specification of the collaborative activities between researchers and research clients (Davison, Martinsons & Kock 2004). For example, action researchers may gain trust from the research clients by providing continuous feedback (Foorthuis & Brinkkemper 2008; Malaurent & Avison 2016). Researchers and research clients may both participate in the scientific publication process (Barata, da Cunha & Melo Santos 2016) or develop a research plan and an organisational improvement plan separately (Moe et al. 2005).

The RCA benefitted this CAR project by serving as a formal recognition of the top management's commitment towards safeguarding employees' anonymity, which increased

employees' confidence when completing the sensitive network questionnaires. Although the effect of the top management's announced commitment on the surveys' response rates was not captured, I believe it mitigated the respondents' concern about anonymity and motivated their participation. Additionally, the collaboration between myself and TTT's top management and the Vice Director of the BSP department was based on mutual trust and understanding. Similar to Malaurent and Avison's (2016) collaborating organisation where research had a high status and recognised their AR as non-consultancy, I found the top management at TTT to be open-minded and receptive to innovations. The General Director at TTT, who represented the top management and held the highest authority in this research, allowed me to conduct the CAR project without requiring me to frequently report to him and to prepare further formal agreements. On this basis, the research client's trust in myself as the researcher had been granted from the outset and this trusting relationship lasted throughout the project.

The informal collaboration between TTT and I accommodated the dynamic nature of CAR and allowed flexible adjustments to the research activities, and it ensured that the research actions were decided based on a consensus between the researcher and the research client. If a formal research process with detailed documentation had been applied for this project, it could have brought adverse effects not aligned with the research client's preferred collaborating style, while producing more paperwork to amend the RCA whenever a change in the activities was required. On this basis, I advise action researchers to prepare an RCA that incorporates the necessary details of the CAR project, while reasonably accounting for the flexibility of CAR and the research client's preferences.

With regard to the use of SNA methods with the CAR approach, Borgatti and Molina (2005) discuss that SNA has powerful applications in the context of action research, yet they also make a cautionary note as top management often want to have access to network data which contains sensitive information about employees. As such, I found the principle of RCA especially critical for CAR which involves network-based interventions. I recommend action researchers employ the measures which were employed in this CAR project to maximise the effectiveness of the SNA methods; an RCA may show the top management's commitment to safeguarding employees' identities during data collection by explicitly specifying that top management will not have access to network data or to anonymised data only.

9.6.2 Cyclical Process Model

The second principle focuses on the planning and execution of the CAR iterations by following the CPM, which involves five stages—diagnosis, action planning, action taking, evaluation and reflection (Davison, Martinsons & Kock 2004). Table 9.6 lists the criteria for the CPM.

Table 9.6. Criteria for the Principle of Cyclical Process Model

2a	Did the project follow the cyclical process model or justify any deviation from it?
2b	Did the researcher conduct an independent diagnosis of the organisational situation?
2c	Were the planned actions based explicitly on the results of the diagnosis?
2d	Were the planned actions implemented and evaluated?
2e	Did the researcher reflect on the outcomes of the intervention?
2f	Was this reflection followed by an explicit decision on whether or not to proceed through an additional process cycle?
2g	Were both the exit of the researcher and the conclusion of the project due to either the project objectives being met or some other clearly articulated justification?

Adopted from Davison, Martinsons and Kock (2004).

As described in Chapters 5 to 8, this CAR project followed the five-stage CPM without any deviation (2a). I also encountered some challenges while following the CPM, which suggest improvements to the CPM as discussed in Section 9.5.2. I performed a diagnosis at the beginning of each stage to understand the current problematic organisational situations, then planned and executed the actions which were followed by the evaluation of the actions' outcomes and a reflection at the end of the stage (2b, 2c, 2d and 2e). The decision on whether to proceed through an additional iteration was elaborated at the end of the evaluation and reflection stage (2f). I also discussed the achievement of both scholarly and business objectives (the latter with the research client) at the end of the evaluation and reflection stage (see Chapter 8), which led to the conclusion of the project (2g).

The principle of CPM provided the project team with a structured process to undertake research activities that contributed to achieving both the practical and scholarly objectives. As the research client had not clearly identified their problem at the beginning of the project, the client and I embarked on a joint co-discovery process. This was in line with other AR projects which allocated much time to clearly understand the problematic situation (see e.g., Huang & Martin-Taylor 2013; Lindgren, Henfridsson & Schultze 2004; Puhakainen & Siponen 2010).

The initial business objective to improve the InfoSec environment was quite vague, which provided the challenge to arrive at specific directions for problem solving. To this end, conducting the risk assessment and discussing with the department managers at the beginning

of the CAR project (see Chapter 5) gave me the essential insights into the problem that TTT was facing. While there is no strict rule pertaining to how many iterations should be in a CAR project (Davison, Martinsons & Kock 2004; Davison, Martinsons & Ou 2012), I advise action researchers to thoroughly diagnose the problematic situation with their collaborating partners as much as possible, which may require using one full iteration if necessary. This supports the researcher's independent diagnosis of the situation and conforms with the principle of CPM to ensure CAR rigour (Davison, Martinsons & Kock 2004). The researcher can make use of the diagnosed findings to refine the planned actions and gain more trust and commitment from the research client by presenting the diagnosed issues to them.

9.6.3 Theory

The third principle focuses on the use of theories to guide research actions and to generate scholarly knowledge from CAR projects (Davison, Martinsons & Kock 2004). Davison, Martinsons and Ou (2012) recommend action researchers to employ focal and instrumental theories, which respectively set the intellectual basis for extending theoretical knowledge and inform research actions. Table 9.7 lists the criteria for the principle of theory.

Table 9.7. Criteria for the Principle of Theory

3a	Were the project activities guided by a theory or set of theories?
3b	Was the domain of investigation, and the specific problem setting, relevant and significant to the interests of the researcher's community of peers as well as the client?
3c	Was a theoretically-based model used to derive the causes of the observed problem?
3d	Did the planned intervention follow from this theoretically-based model?
3e	Was the guiding theory, or any other theory, used to evaluate the outcomes of the intervention?

Adopted from Davison, Martinsons and Kock (2004).

In line with Davison, Martinsons and Ou's (2012) recommendation, I employed multiple focal and instrumental theories throughout this project (3a). These theories were the theory of social power bases (Raven 2008), opinion leadership theory (Liu et al. 2017; Valente & Davis 1999), theory of climate formation (Ashforth 1985; Schneider & Reichers 1983), graph theory (Barnes & Harary 1983), experiential learning cycle-based approach for InfoSec training (Karjalainen & Siponen 2011) and the critical elements for InfoSec training which were drawn from my literature review. This project's domain of investigation and problem setting are relevant to the behavioural InfoSec field. This was established through my review of the relevant literature presented in Chapter 2. The acceptance of several of my research articles for publications in peer-reviewed journals and conference proceedings in the information systems field during the

CAR process provides evidence for the project's relevancy and significance to the scientific community (3b).

The nature of this CAR project was exploratory at the beginning, where I performed a risk assessment to diagnose the problematic InfoSec situation at TTT and found the primary issue to be employees' inadequate InfoSec awareness. Many of the identified vulnerabilities were about the lack of InfoSec training and InfoSec communication between employees. Based on the risk assessment's result, I used the theoretical model of climate formation (Ashforth 1985; Schneider & Reichers 1983) to explain the relationship between the lack of InfoSec-related socialisation and the previously poor InfoSec climate at TTT (i.e., employees' failure to see the priority of InfoSec in the workplace) (3c). The main intervention (i.e., the diffusion of InfoSec knowledge by the champions) was planned to increase the InfoSec-related socialisation and improve the InfoSec climate in line with the mentioned theoretical model (3d). The achievement of the scholarly objective through the intervention, which aimed at identifying the mechanisms and factors of InfoSec climate formation, was evaluated by examining the theoretical model of such formation (3e).

As the CAR project developed, the decisions to undertake research actions resulted in the adoption of further focal and instrumental theories which I had not planned for or considered at the beginning of the project. Opinion leadership theory (Liu et al. 2017; Valente & Davis 1999) and the theory of social power bases (Raven 2008) were incorporated to guide the selection of influential InfoSec champions in the action planning stage. This only emerged after the diagnosis stage's evaluation and reflection as described in Chapter 5. Without considering the context, the selection of InfoSec champions had little relevance to the initial scholarly objective to understand the formation of an InfoSec climate. However, the examination of these theories, as part of the action planning stage described in Chapter 6, produced additional insights into the applications of SNA in behavioural InfoSec research and contributed knowledge to the unexplored area of using opinion leaders for InfoSec management. Therefore, I confirm Davison, Martinsons and Kock's (2004) advice that action researchers should remain flexible and genuinely interested in enhancing the organisational situation, which allows for making adjustments to the research activities that lead to unexpected discovery of knowledge. My experience of the progressive adoption of theories in this CAR project also reflects the argument that it is challenging to determine a suitable theory at the beginning of an AR (Vidgen, Madsen & Kautz 2004).

9.6.4 Change through Action

The fourth principle focuses on the mutual understanding between action researchers and research clients about the organisational situation, its improvement and the undertaking of actions to achieve this improvement (Davison, Martinsons & Kock 2004). This principle offers a checklist of five questions listed in Table 9.8.

Table 9.8. Criteria for the Principle of Change through Action

4a	Were both the researcher and client motivated to improve the situation?
4b	Were the problem and its hypothesised cause(s) specified as a result of the diagnosis?
4c	Were the planned actions designed to address the hypothesised cause(s)?
4d	Did the client approve the planned actions before they were implemented?
4e	Was the organisation situation assessed comprehensively both before and after the intervention?
4f	Were the timing and nature of the actions taken clearly and completely documented?

Adopted from Davison, Martinsons and Kock (2004).

In the initial meeting and through the diagnosis, which were described in Chapters 4 and 5 respectively, TTT and I established our motivation to improve the InfoSec environment at TTT (4a). The major problem was identified as employees' inadequate InfoSec awareness, and its hypothesised causes as determined from the risk assessment described in Chapter 4 included employees' lack of InfoSec-related socialisation and InfoSec training (4b). The plan to address the identified problem was to have InfoSec champions carry out a diffusion of InfoSec knowledge to increase InfoSec-related socialisation and to provide InfoSec training (4c). The diffusion plan, which followed the train the trainers approach, was agreed between top management and the project team at the end of the diagnosis stage (see Chapter 5) (4d). The InfoSec-related networks before and after the champions' diffusion of InfoSec knowledge were comprehensively evaluated by the performance of SNA as described in Chapters 6 and 8 (4e). The project's actions in the four CAR stages were presented in the respective chapters of this thesis and a timeline of the project was documented and provided in Chapter 3 (4f).

To satisfy criteria 4b, 4c and 4d, the project team and top management followed a collaborative procedure in each stage to ensure that all actions supporting the main intervention, such as determining the selection criteria for champions (see Chapter 6) and designing and implementing the training for the champions (see Chapter 7) were thoroughly discussed and agreed upon before being carried out. Specifically, I discussed the actions for each stage with the Vice Director of the BSP department and, on occasion, with top management either in-person or in online meetings throughout the CAR project. At the end of the meetings when

agreements on actions were achieved, we summarised the agreements in emails and we kept these as meeting records. Moreover, the project team orally presented the stages' outcomes and the follow-up actions in the milestone meetings with top management at the end of each stage. In these milestone meetings, the project team sought support from top management if needed, such as requesting the General Director to announce the commitment towards safeguarding employees' anonymity for the data collection. Top management acknowledged the achieved outcomes at the end of the milestone meetings and gave permission for the project to proceed further or conclude.

Although this CAR project did not encounter any major problems with the agreed collaboration style between myself and TTT, our communication failed at least once when top management decided to launch the InfoSec event without informing me in advance (see Section 8.1). This initiative of top management was carried out with the good intention of facilitating discussions about InfoSec matters among employees and supporting the CAR project. However, it also indicated that top management may not have fully appreciated the importance of maintaining effective communication and synergy between the researcher and the research client in a CAR project. I recognise this incident as a drawback of the informal collaboration style between myself and TTT and action researchers are advised to be aware of this potential issue.

9.6.5 Learning through Reflection

The fifth principle focuses on the action researchers' responsibilities to inform research clients about the project's progress and to report research findings, which may take the form of research publications (Davison, Martinsons & Kock 2004). Moreover, this principle covers the reflection and learning which concern further actions in the focal context, actions in related research domains, theory and the suitability of the CAR methodology (Davison, Martinsons & Kock 2004). Table 9.9 lists the criteria for the principle of learning through reflection.

Table 9.9. Criteria for the Principle of Learning through Reflection

5a	Did the researcher provide progress reports to the client and organisational members?
5b	Did both the researcher and the client reflect upon the outcomes of the project?
5c	Were the research activities and outcomes reported clearly and completely?
5d	Were the results considered in terms of implications for further action in this situation?
5e	Were the results considered in terms of implications for action to be taken in related research domains?
5f	Were the results considered in terms of implications for the research community (general knowledge, informing/re-informing theory)?
5g	Were the results considered in terms of the general applicability of CAR?

Adopted from Davison, Martinsons and Kock (2004).

As described in Section 9.6.4, progress reports were orally presented to top management and the project team in the milestone meetings at the end of the stages (5a). Reflections on the outcomes of the stages were mainly performed by myself as the researcher and the Vice Director of the BSP department and occasionally with top management (5b). Meeting minutes, which documented the results and action plan that resulted from the reflection of each stage, were sent as emails to the project stakeholders. The research activities and outcomes were clearly and completely reported in this thesis and were published separately in the form of research publications (5c). Top management at TTT did not require any written reports; the project team orally presented the research activities and outcomes to top management in the milestone meetings at the end of the stages.

Throughout this CAR project, TTT received a number of practical benefits such as improving their understanding about InfoSec implementation and InfoSec risk assessment, a group of experienced InfoSec champions for future diffusion of InfoSec knowledge and increasing the InfoSec-related socialisation among employees. TTT can leverage these resources acquired from this CAR project to take further actions to improve their InfoSec environment, which potentially involve periodically conducting risk assessments and training the next group of InfoSec champions (5d). Since the Vice Director of the BSP department participated in the research actions and now holds the relevant materials (e.g., risk assessment spreadsheet and selection criteria for champions), it is possible for TTT to perform these actions in the future without my support.

Organisational and theoretical contributions to the related behavioural InfoSec domain were discussed in Sections 9.3 and 9.4 (5e and 5f). Specifically, my research demonstrated the practical applications of SNA for conducting InfoSec risk assessment and improving InfoSec communication and influence in the workplace, especially by identifying InfoSec champions to diffuse InfoSec knowledge. Theoretical implications included the extension of current knowledge about the formation of InfoSec climate, the determinants of employees' InfoSec influence and various future research directions. The general applicability of the CAR approach, which encompasses its benefits and limitations in this project's context, and the methodological contributions to the community of action researchers (Davison, Martinsons & Kock 2004) are discussed in Sections 9.5 (5g).

Overall, this project benefitted from adopting the CAR approach, especially from the researcher–client collaborative process and the CPM. By collaborating with TTT to achieve

the business objective, I received unexpected opportunities to advance knowledge about the application of SNA methods in improving an InfoSec environment and about the determinants of InfoSec influence. Had this research only analysed the longitudinal formation of an InfoSec climate in a workplace without performing any network-based interventions to improve it, such opportunities to advance knowledge would not have been presented. Moreover, the CPM effectively served as a guideline for the project team to systematically achieve the practical goals of each stage and of the iteration, while ensuring the generation of scholarly knowledge through reflecting on the focal and instrumental theories. The adoption of a CAR approach in this research requests concrete interventions (e.g., the network-based risk assessment and the champions' diffusion of InfoSec knowledge) to improve the organisational situation. Thus, the research findings derived from this CAR project might not accurately reflect the phenomena in a workplace without interventions. However, performing the interventions enabled me to extend on the existing knowledge through reflection on the results of the interventions.

9.7 Limitations

The limited time frame had some consequences, which is a common issue of CAR projects conducted as part of a PhD candidature (Avison, Davison & Malaurent 2017). As discussed in Section 9.5, the evaluation of the intervention performed in this CAR project focused on the changes in the InfoSec-related networks, which reflected the increased levels of employees' provisions of InfoSec support and InfoSec influence. I was not able to collect evidence which indicated changes in the organisational InfoSec, such as the levels of InfoSec awareness and InfoSec compliance, or the number of InfoSec risks and InfoSec incidents. While we expected that the improved InfoSec-related socialisation would subsequently improve organisational InfoSec, as confirmed in prior studies (e.g., Herath & Rao 2009b; Safa et al. 2015; Warkentin, Johnston & Shropshire 2011), it would have been useful to examine the relationship between network measures and other non-network metrics about organisational InfoSec.

I also did not conduct qualitative interviews with the champions after the change program to gather rich and in-depth data about their experience during the diffusion of InfoSec knowledge. This was due to both the project's limited time frame and the project's scholarly and business objectives which did not focus on the champions' behaviours during the diffusion. Had such data been collected, this research could have offered further lessons learned concerning the champions' challenges and their responses to these challenges during the diffusion.

9.8 Future Directions for Research

This section outlines the directions for future research based on the organisational, theoretical and methodological contributions that were discussed in sections 9.3, 9.4 and 9.5 respectively. In line with my recommendation to adopt SNA methods for analysing InfoSec risks, future research is encouraged to further analyse InfoSec risk networks in different organisational contexts to reveal the common patterns of how the vulnerabilities and threats are tied to each other. This can potentially extend theoretical knowledge about the relational nature of InfoSec risks. Acquiring such knowledge enables the development of better practices which can efficiently and effectively mitigate organisational InfoSec risks by removing those commonly identified as the root causes in the risk networks.

Throughout this CAR project and in section 9.3, I have demonstrated and elaborated on the practical use of network-based interventions and network measures as quantitative metrics for improving organisational InfoSec. Additionally, I recommended organisations to align their network-based interventions with the strategic objectives and current structures of their InfoSec-related networks. To this end, it would be desirable to have a framework which informs organisations about the strategic advantages and disadvantages of their current InfoSec-related network structures, then recommends the suitable interventions to improve the organisations' InfoSec environments. The development of such a framework demands future research further investigate InfoSec-related networks in different industries and cultural settings and analyse how the unique structures of these networks impact on organisations' InfoSec.

Consistent with Gesell, Barkin and Valente's (2013) discussion that the thresholds for network measures vary according to the change program's targets, network-based interventions in the InfoSec context might have their unique optimal thresholds for network measures as well. Determining these optimal thresholds allows organisations to devise new network-based interventions to improve their InfoSec environments. On this basis, my research serves as the first study to evaluate InfoSec-related networks based on a set of network measures. Future research is encouraged to employ similar measures to further evaluate the InfoSec-related networks and accumulative findings from multiple evaluations may reveal the optimal thresholds for network measures in the InfoSec context.

In addition to network centrality which indicates the influential status of InfoSec champions, as discussed in section 9.4, I encourage future studies to examine employees' brokerage roles on their provisions of InfoSec support and InfoSec influence, and on their InfoSec perceptions and behaviours. Brokerage roles refer to employees' advantageous positions in the networks which allow them to have access to unique resources and to control the flows of resources between groups (Bruque, Moyano & Eisenberg 2009; Burt, Kilduff & Tasselli 2013; Carpenter, Li & Jiang 2012; Rowley 1997; Wellman 1983). Employees who can broker organisational resources are influential in the workplaces. Unlike centrality measures, which only reflect the positions and connections of an employee, brokerage roles take into account employees' department or group memberships. On this basis, social network theory classifies five types of brokerage roles in a network—'coordinator', 'consultant' or 'itinerant', 'gatekeeper', 'representative' and 'liaison' (Gould & Fernandez 1989; Hanneman & Riddle 2005).

These brokerage roles of the nodes representing employees are visualised in Figure 9.3. The shapes of the nodes denote their department memberships—nodes having the same shapes also work in the same departments. For example, when employee B bridges the flow of resources between employee A and employee C and the three of them work in the same department, then employee B is described as holding the 'coordinator' role in this situation. As a resource broker between employee A and employee C, employee B can hold a 'consultant' role, a 'gatekeeper' role or a 'representative' role when there is a same-department relationship between A and C, between B and C or between A and B (see Figure 9.3). Finally, when B helps A transfer their resources to C and the three of them work in different departments, then B serves as a 'liaison' for A and C.

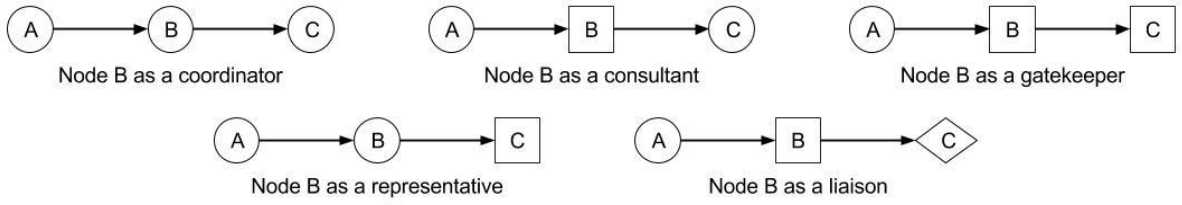


Figure 9.3. Brokerage Roles

Adapted from Hanneman and Riddle (2005).

I expect that these brokerage roles of employee B will have different impacts on their InfoSec influence. Similarly, employees who hold different brokerage roles might also have distinctive background characteristics and behaviours. For example, a liaison who can transfer resources

across different departments can be assumed to have greater influence than a coordinator who can circulate resources only among colleagues in the same department. Gaining the knowledge about the impacts of brokerage roles on InfoSec influence may lead to further classification of different InfoSec champions. For example, employees with coordinator and gatekeeper roles might be selected to be local champions, and employees with consultant and liaison roles might be selected to be champions who diffuse InfoSec-related resources across organisational functions.

The project team recognised the importance of non-network factors as we discussed with the champions their concerns after the training workshops. Some champions reported that they lacked confidence in their communication and leadership skills to influence other employees' InfoSec behaviours. This finding supports the fact that the recruitment of champions for information systems-related change programs does not solely rely on their network measures (Greenhalgh et al. 2004; Jenssen & Jørgensen 2004). Prior studies about opinion leadership have identified important personal characteristics of effective champions which include being politically savvy, self-confidence, willing to take calculated risks, energetic and enthusiastic, persistent and knowledgeable, just to name a few (Howell & Boies 2004; Howell & Higgins 1990; Jenssen & Jørgensen 2004; Martinsons 1993).

In the InfoSec context there has been little research to determine the non-network attributes of InfoSec champions. My research findings extend current knowledge about the determinants of InfoSec influence and can be used to select InfoSec champions in practice. Of the few studies that determine the attributes of InfoSec champions, Martinez-Moyano et al. (2008) identify InfoSec champions as end-users who actively reported system problems to systems administrators. The roles and required abilities of InfoSec champions can be more sophisticated, as Everett (2010) discusses the InfoSec champions' abilities of being able to provide other employees with information and materials about InfoSec matters and to facilitate discussions about InfoSec issues. Gabriel and Furnell (2011) argue that some employees possess specific personality traits suited for InfoSec champions, such as imagination and altruism, and propose to use personality tests to identify champions.

While I was aware of these non-network factors that can increase an employee's potential to be InfoSec champion, examining these attributes' effects was outside my research scope. Future studies can perform SNA to test hypotheses about the impacts of these non-network attributes on employees' provisions of InfoSec support and InfoSec influence, which are

conceptualised as network ties. Further, I noted in Section 9.3.2 that some of employees' non-network attributes such as gender and age were negated when the network's structural mechanisms were accounted for. Therefore, future studies are encouraged to replicate my study in other work settings to determine selection criteria that remain valid across different network structures.

This research is the first empirical study to employ a longitudinal SNA method to investigate the formation of an InfoSec climate. Since climate is argued to be the surface-level manifestation of how things are done in an organisation, studying the formation of InfoSec climate gives cues to the development of InfoSec culture (Kuenzi & Schminke 2009; Schneider, Ehrhart & Macey 2011). These cues help organisations develop InfoSec culture by altering the changeable workplace features which impact InfoSec climate such as employees' socialising patterns. Therefore, it is worth pursuing the research direction to explore the forming mechanisms of an InfoSec climate from the network perspective. However, the current understanding about the formation of an InfoSec climate is still in its infancy. I discuss future research directions to extend the theoretical knowledge about InfoSec climate below.

The research findings in this CAR project about the mechanisms and factors which contributed to the formation of an InfoSec climate were examined when the intervention took place. As such, the forming process described in this research might not accurately reflect the natural formation of an InfoSec climate, which may also occur at a slower rate without the increased InfoSec-related socialisation caused by the champions' diffusion of InfoSec knowledge. I recommend future behavioural InfoSec research to analyse the formation of an InfoSec climate in a workplace where InfoSec-related socialisation and InfoSec influence are not affected by any interventions. Findings from these studies would deepen the understanding about the natural formation of an InfoSec climate.

The finding indicating climate perceptions of direct supervisors' InfoSec behaviours were unaffected by social influence suggests that different types of climate perceptions have their unique forming mechanisms. For example, the formation of this climate perception might be affected by other types of socialisation which my study did not capture. This climate perception may also be influenced by indirect comparison which explains that actors with similar positions in the network tend to behave or think similarly, rather than by direct socialisation such as provisions of organisational resources (Leenders 2002). Employees might develop their own climate perception of direct supervisors' InfoSec behaviours independently to their colleagues'

social influence as well. Therefore, it is necessary and helpful to determine the alternative forming mechanisms of climate perceptions.

Ashforth (1985) discusses that the formation of an organisational climate can be influenced by the corporate culture and the work setting of employees. Employees' sense-making activities and social influence, which contribute to the development of climate perceptions, can be affected by the different organisational cultures that determine employees' values and assumptions (Ashforth 1985). Moreover, features of the physical environment such as walls and offices can either facilitate or discourage employees' interactions and other sense-making activities which give rise to a shared climate (Ashforth 1985).

All three offices of TTT (headquarters, architect and factory offices) had an open office space with few walls and partitions. Although TTT has a flat organisational culture, the Vietnamese culture in general has high collectivism and large power distance which respectively encourage achieving consensus and discourage challenging authority (Hofstede 2001). Thus, I argue that the confirmed effect of social influence on employees' formation of climate perceptions of their colleagues' InfoSec behaviours might be affected by TTT's physically open work environment and the Vietnamese culture. Further, the action planning stage's analysis of the network visualisations showed that employees from departments such as project management and construction together formed a large cluster in TTT due to their job duties which were heavily related to each other. As such, I propose that having related job duties can also contribute to the formation of organisational climate, extending Ashforth's (1985) theory. This proposed effect is in line with the theory of homophily which posits that similar individuals tend to associate and interact more with each other (McPherson, Smith-Lovin & Cook 2001). Future studies should endeavour to empirically validate these discussed effects of national culture, physical environment and job duties on the formation of an InfoSec climate.

In line with Ashforth's (1985) discussion about the work setting and organisational culture affecting the formation of climate, I further posit that the structures of employees' networks, which are the consequences of the physical environment and work culture, can also govern the formation of an InfoSec climate. The finding in this CAR project that employees developed favourable climate perceptions of colleagues' InfoSec behaviours was confirmed at the same time as the InfoSec-related networks had their structural features improved. While there lacked the statistical evidence to support the causal relationship between the improved network structures and the formation of InfoSec climate, I propose that the formation of a favourable

InfoSec climate can be facilitated by the increases in the InfoSec-related networks' density, reciprocity and transitivity and by the decrease in these networks' centralisation.

Prior studies have examined the effects of these network structures on various organisational outcomes with conflicting results (Balkundi & Harrison 2006). Some argued that having high density values can lead to desirable organisational outcomes such as better transfer of knowledge and group performance (Bruque, Moyano & Eisenberg 2009; Burt 2000; Reagans & Zuckerman 2001; Sparrowe et al. 2001). Others stated that dense networks result in redundant knowledge, offer less information advantage and negatively affect productivity (Balkundi & Harrison 2006; Burt 2000; Gould 1993; Zhou, Siu & Wang 2010). In the context of an InfoSec climate, having high density may or may not be desirable for the formation of an InfoSec climate. For example, it can be reasoned that higher density values of the InfoSec support network result in more employees exerting InfoSec influence over each other, thereby accelerating the formation of an InfoSec climate. Conversely, too much provision of InfoSec support may create the common belief that InfoSec is part of the expected background (Furnell & Thomson 2009) and employees might stop realising a favourable InfoSec climate in the workplace. Analysing the relationship between network structures and the formation of an InfoSec climate advances theoretical knowledge about the desirable and undesirable network structures in the InfoSec context.

Currently, there are few studies on organisational information systems which explicitly report the use of SNA methods. Action researchers employed SNA methods to improve collaboration in software process improvement (Nielsen & Tjørnehøj 2005, 2010) and to develop knowledge management systems (Butler et al. 2008). My literature review did not find many behavioural InfoSec studies which performed SNA, much less using SNA methods with an AR approach. Lee (2010) and Davison (2010) argue that SNA is not even accurately understood by information systems researchers as many of them do not use the term 'social network' with its scientific meaning from sociology. There are an increasing number of studies which focus on the use of SNA methods for designing and implementing organisational change programs (e.g., Cross, Parker & Borgatti 2002; Gesell, Barkin & Valente 2013; Hatala & Lutta 2009; Parise 2007; Valente 2012), however, not many of these studies follow AR designs and they put emphasis on the practicality of the studied network-based interventions, but not on their theoretical contributions. In contrast, AR strives to achieve both the goals of practically

improving the organisational situations and generating scholarly knowledge (Baskerville & Myers 2004; Davison, Martinsons & Ou 2012).

The project team for this study evaluated the improvements which focused on the InfoSec-related networks. Other benefits concerning organisational InfoSec, such as the mitigation of InfoSec risks or reduction of InfoSec violations, were anticipated as results of the improved InfoSec-related networks which facilitated more provision of InfoSec support and InfoSec influence. If employees provide each other with more InfoSec support and influence each other to improve InfoSec behaviours, they may become more aware of InfoSec matters and the number of InfoSec risks and violations at TTT may decrease. Due to the short time frame and limited access to TTT's records of InfoSec incidents, the evaluation of the intervention's impacts on organisational InfoSec was not possible in this project. If the project's time frame could be extended, it would be useful to study the relationships between the mentioned possible benefits and the improved InfoSec-related networks.

There are, therefore, opportunities to further explore the benefits of combining the two research streams—that is, conducting action researches which employ network-based interventions to practically improve organisational situations, while theorising these interventions' process and outcome. For example, Valente (2012) discusses that studies involving network-based interventions concern not only individual behaviours (e.g., whether the individuals perform or receive the diffusion or not), but also the system dynamics which reflect how communities respond to the interventions by changing their patterns of interactions. Likewise, researchers may arrive at process theories of how champions and non-champions change their interactions during an intervention by employing SNA methods in information systems- or InfoSec-related AR projects. To this end, my research provides one of the first examples of demonstrating the use of SNA methods in an InfoSec-related CAR project, in a context where the methodological contributions of SNA methods to InfoSec-related AR have not been fully explored. Although the InfoSec training delivered during the action taking stage was not the emphasis of this CAR project, future action research can empirically appraise the adjusted experiential learning cycle-based InfoSec training approach in their contexts as well.

9.9 Conclusion

At the end of this CAR project I have achieved my scholarly objective and answered the two research questions stated at the beginning of the thesis, which aimed at understanding the

formation of an InfoSec climate and exploring the applications of SNA methods for improving organisational InfoSec. The research outcomes also satisfied the business objective of TTT to improve their InfoSec environment. The CAR project successfully involved all stakeholder groups at TTT, including top management, department managers and employees at three locations, in an organisation-wide InfoSec change program unprecedented in TTT. The CAR project provided the procedures and materials for conducting future risk assessments at TTT and a group of champions, who have undergone InfoSec training and experienced in the diffusion of InfoSec knowledge, was established. As a result, the CAR project improved the organisational situation at TTT and the stakeholders there are prepared to continuously enhance the InfoSec environment.

In terms of organisational contributions, this research demonstrated the application of SNA methods for conducting InfoSec risk assessment and for evaluating and improving an InfoSec environment with network-based interventions. Moreover, this research offered a list of theoretically-based criteria for selecting influential InfoSec champions to diffuse InfoSec knowledge in a workplace. This research offered theoretical contributions by extending current knowledge about the determinants of InfoSec influence and about the formation of an InfoSec climate. My reflection on the process of conducting this CAR project offered methodological contributions on the combined use of SNA methods and the CAR approach. I recommend action researchers to capitalise on the features of SNA methods to enhance the rigour and success of CAR, such as using network visualisations to communicate with the research clients or designing network-based interventions and quantitatively evaluating the outcomes with network measures.

My experience of conducting this CAR project suggests the need for action researchers to maintain flexibility throughout the research process, which enables the effective combination of theories and methods to improve a problematic organisational situation and to produce scholarly knowledge. I proposed improvements to the CAR process which involve developing a collaborative space and identifying research ideas and real-world problems before commencing a CAR project. I also discussed the potential criteria and considerations for selecting theories and the need to prepare contingency actions for the undesirable situations that might occur in a CAR. For CAR projects that collect sensitive data about employees' networks to perform SNA, the RCA holds a critical role in establishing the researcher–practitioner agreements and commitments towards safeguarding participants' anonymity. In

this context, an RCA ensures the ethical use of SNA methods and increases the network survey's response rate by improving participants' confidence in answering the survey.

As a final reflection of this thesis, I found that conducting CAR offers benefits to researchers, academia and the industry. As the action researcher who performed the whole CAR project I benefitted from the research process which developed my abilities to effectively liaise with industry partners and to creatively employ multiple research methods to achieve both scholarly and business objectives. I have also built up a strong collaborative relationship with the industry partner which lasts beyond the end of this project. The CAR approach allows theoretical ideas and existing tools to be validated in practical contexts while industry partners can improve their practices, thus narrowing the gap between theory and practice.

References

Adamic, LA & Glance, N 2005, 'The political blogosphere and the 2004 U.S. election: divided they blog', in *Proceedings of the 3rd international workshop on Link discovery - LinkKDD '05*, pp. 36–43 (doi: 10.1145/1134271.1134277).

Adams, A & Sasse, M 1999, 'Users are not the enemy', *Communications of the ACM*, vol. 42, no. 12, pp. 40–46.

Adams, P 2006, 'Exploring social constructivism: theories and practicalities', *Education 3-13*, vol. 34, no. 3, pp. 243–257 (doi: 10.1080/03004270600898893).

Ahuja, MK & Carley, KM 1998, 'Network structure in virtual organizations', *Journal of Computer-Mediated Communication*, vol. 3, no. 4 (doi: 10.1111/j.1083).

Ajzen, I 2011a, 'The theory of planned behaviour: reactions and reflections', *Psychology & Health*, vol. 26, no. 9, pp. 1113–1127 (doi: 10.1080/08870446.2011.613995).

Ajzen, I 2011b, 'The theory of planned behavior', in PAM Van Lange, AW Kruglanksi & ET Higgins (eds), *Handbook of theories of social psychology: volume one*, SAGE Publications, pp. 438–459.

Akella, D 2010, ‘Learning together: Kolb’s experiential theory and its application’, *Journal of Management and Organization*, vol. 16, no. 1, pp. 100–112 (doi: 10.5172/jmo.16.1.100).

Albrechtsen, E 2007, ‘A qualitative study of users’ view on information security’, *Computers & Security*, vol. 26, no. 4, pp. 276–289 (doi: 10.1016/j.cose.2006.11.004).

Albrechtsen, E & Hovden, J 2009, ‘The information security digital divide between information security managers and users’, *Computers and Security*, vol. 28, no. 6, pp. 476–490 (doi: 10.1016/j.cose.2009.01.003).

Albrechtsen, E & Hovden, J 2010, ‘Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study’, *Computers & Security*, vol. 29, no. 4, pp. 432–445 (doi: http://dx.doi.org/10.1016/j.cose.2009.12.005).

Alhogail, A. 2015, ‘Design and validation of information security culture framework’, *Computers in Human Behavior*, vol. 49, pp. 567–575 (doi: https://doi.org/10.1016/j.chb.2015.03.054).

Alvesson, M & Kärreman, D 2007, ‘Constructing mystery: empirical matters in theory development’, *Academy of Management Review*, vol. 32, no. 4, pp. 1265–1281.

Alvesson, M & Sandberg, J 2011, ‘Generating research questions through problematization’, *Academy of Management Review*, vol. 36, no. 2, pp. 247–271.

Anderson, JM 2003, ‘Why we need a new definition of information security’, *Computers & Security*, vol. 22, no. 4, pp. 308–313 (doi: http://dx.doi.org/10.1016/S0167-4048(03)00407-3).

Anderson, R & Moore, T 2009, ‘Information security: where computer science, economics and psychology meet’, in *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 367, no. 1898, pp. 2717–2727 (doi: 10.1098/rsta.2009.0027).

Arbuckle, JL 2011, *IBM SPSS® Amos™ 20 user's guide*, Amos Development Corporation, <ftp://public.dhe.ibm.com/software/analytics/spss/documentation/amos/20.0/en/Manuals/IBM_SPSS_Amos_User_Guide.pdf>.

Ashenden, D 2008, 'Information security management: a human challenge?', *Information Security Technical Report*, vol. 13, no. 4, pp. 195–201 (doi: 10.1016/j.istr.2008.10.006).

Ashforth, B 1985, 'Climate formation: issues and extensions', *Academy of Management Review*, vol. 10, no. 4, pp. 837–847.

Avison, DE, Baskerville, RL & Myers, MD 2001, 'Controlling action research projects', *Information Technology & People*, vol. 14, no. 1, pp. 28–45.

Avison, DE, Davison, RM & Malaurent, J 2017, 'Information systems action research: debunking myths and overcoming barriers', *Information & Management*, pp. 1–11 (doi: 10.1016/j.im.2017.05.004).

Avison, D, Lau, F, Myers, M & Nielsen, PA 1999, 'Action research', *Communication of the ACM*, vol. 42, no. 1, pp. 94–97 (doi: 10.1145/291469.291479).

Aytes, K & Connolly, T 2004, 'Computer security and risky computing practices', *Journal of Organizational and End User Computing*, vol. 16, no. 3, pp. 22–40 (doi: 10.4018/joeuc.2004070102).

Balkundi, P & Harrison, DA 2006, 'Ties, leaders, and time in teams: strong Inference about the effects of network structure on team viability', *Academy of Management Journal*, vol. 49, no. 1, pp. 49–68 (doi: 10.2307/20159745).

Ballabio, G 2013, 'Security and availability techniques for cloud-based applications', *Computer Fraud & Security*, vol. 2013, no. 10, pp. 5–7 (doi: http://dx.doi.org/10.1016/S1361-3723(13)70091-5).

Barata, J, da Cunha, PR & Melo Santos, AP 2016, 'Mind the gap: assessing alignment between hospital quality and its information systems', *Information Technology for Development*, pp. 1–18 (doi: 10.1080/02681102.2016.1197173).

Barkley, EFK, Cross, P & Major, CH 2005, *Collaborative learning techniques: a handbook for college faculty*, Jossey-Bass, San Francisco, CA.

Barlow, JB, Warkentin, M, Ormond, D & Dennis, AR 2013, 'Don't make excuses! Discouraging neutralization to reduce IT policy violation', *Computers & Security*, vol. 39, pp. 145–159.

Barnes, JA 1954, 'Class and committees in a Norwegian island parish', *Human Relations*, vol. 7, no. 1, pp. 39–58 (doi: 10.1177/001872675400700102).

Barnes, JA & Harary, F 1983 'Graph theory in network analysis', *Social Networks*, vol. 5, no. 2, pp. 235–244 (doi: 10.1016/0378-8733(83)90026-6).

Barqawi, N, Syed, K & Mathiassen, L 2016, 'Applying service-dominant logic to recurrent release of software: an action research study', *Journal of Business & Industrial Marketing*, vol. 31, no. 7, pp. 928–940 (doi: 10.1108/JBIM-02-2015-0030).

Bartnes, M, Moe, NB & Heegaard, PE 2016, 'The future of information security incident management training: a case study of electrical power companies', *Computers & Security*, vol. 61, pp. 32–45 (doi: http://dx.doi.org/10.1016/j.cose.2016.05.004).

Baskerville, RL 1999, 'Investigating information systems with action research', *Communications of AIS*, vol. 2, p. 4, <http://aisel.aisnet.org/cais/vol2/iss1/19>.

Baskerville, RL & Myers, MD 2004, 'Special issue on action research in Information systems: making IS research relevant to practice: foreword', *MIS Quarterly*, vol. 28, no. 3, pp. 329–335.

Baskerville, RL, Park, E & Kim, J 2014, 'An emote opportunity model of computer abuse', *Information Technology & People*, vol. 27, no. 2, pp. 1–31.

Baskerville, RL & Siponen, M 2002, 'An information security meta-policy for emergent organizations', *Logistics Information Management*, vol. 15, no. 5/6, pp. 337–346 (doi: 10.1108/09576050210447019).

Baskerville, RL & Wood-Harper, A 1998, 'Diversity in information systems action research methods', *European Journal of Information Systems*, vol. 7, no. 2, pp. 90–107 (doi: 10.1057/palgrave/ejis/3000298).

Bastian, M, Heymann, S & Jacomy, M 2009, 'Gephi: an open source software for exploring and manipulating networks', in *International AAAI conference on weblogs and social media*, <https://www.aaai.org/ocs/index.php/ICWSM/09/paper/view/154/1009>.

Becker, I & Sasse, MA 2017, 'Finding security champions in blends of organisational culture', in *Proceedings of the 2nd European workshop on usable security - EuroUSEC '17* (doi: 10.14722/eurousec.2017.23007).

Blake, A 2016, 'Cyberattack claims multiple airports in Vietnam', *The Washington Times*, 29 July 2016, viewed 14 November 2017, <http://www.washingtontimes.com/news/2016/jul/29/cyberattack-claims-multiple-airports-vietnam-airli/>.

Blake, R & Ayyagari, R 2012, 'Analyzing information systems security research to find key topics, trends, and opportunities', *Journal of Information Privacy & Security*, vol. 8, no. 3, pp. 37–67 (doi: 10.1080/15536548.2012.10845660).

Blakley, B & Mcdermott, E 2002, 'Information security is information risk management', in *Proceedings of the 2001 workshop on new security paradigms*, ACM, New York, NY, pp. 97–104.

Boer, H, Seydel, ER & Norman, P 1996, 'Protection motivation theory', in M Conner and P Norman (eds), *Predicting health behaviour: research and practice with social cognition models*, Open University Press, Maidenhead, UK, pp. 95–120.

Boghossian, P 2006, 'Behaviorism, constructivism, and Socratic pedagogy', *Educational Philosophy and Theory*, vol. 38, no. 6, pp. 713–722 (doi: 10.1177/1469787408100194).

Bojanc, R & Jerman-Blažič, B 2008, 'An economic modelling approach to information security risk management', *International Journal of Information Management*, vol. 28, no. 5, pp. 413–422 (doi: http://dx.doi.org/10.1016/j.ijinfomgt.2008.02.002).

Bollen, KA & Stine, RA 1992, 'Bootstrapping goodness-of-fit measures in structural equation models', *Sociological Methods & Research*, vol. 21, no. 2, pp. 205–229 (doi: 10.1177/0049124192021002004).

Borgatti, SP 2005, ‘Centrality and network flow’, *Social Networks*, vol. 27, no. 1, pp. 55–71 (doi: 10.1016/j.socnet.2004.11.008).

Borgatti, SP & Cross, R 2003, ‘A relational view of information seeking and learning in social networks’, *Management Science*, vol. 49, no. 4, pp. 432–445 (doi: 10.1287/mnsc.49.4.432.14428).

Borgatti, SP, Everett, MG & Freeman, LC 2002, ‘Ucinet for Windows: software for social network analysis’, Analytic Technologies, Harvard, MA.

Borgatti, SP, Everett, MG & Johnson, JC 2013, *Analyzing social networks*, SAGE Publications.

Borgatti, SP & Foster, P 2003, ‘The network paradigm in organizational research: a review and typology’, *Journal of management*, vol. 29, no. 6, pp. 991–1013.

Borgatti, SP & Molina, JL 2005, ‘Toward ethical guidelines for network research in organizations’, *Social Networks*, vol. 27, no. 2, pp. 107–117 (doi: 10.1016/j.socnet.2005.01.004).

Börjesson, A, Martinsson, F & Timmerås, M 2006, ‘Agile improvement practices in software organizations’, *European Journal of Information Systems*, vol. 15, no. 2, pp. 169–182 (doi: 10.1057/palgrave.ejis.3000603).

Boss, SR, Kirsch, LJ, Angermeier, I, Shingler, RA & Boss, RW 2009, ‘If someone is watching, I’ll do what I’m asked: mandatoriness, control, and information security’, *European Journal of Information Systems*, vol. 18, no. 2, pp. 151–164.

Bott, E 1955, ‘Urban families: conjugal roles and social networks’, *Human Relations*, vol. 8, no. 4, pp. 345–384 (doi: 10.1177/001872675500800401).

Bradbury-Huang, H 2010, ‘What is good action research?: why the resurgent interest?’, *Action Research*, vol. 8, no. 1, pp. 93–109 (doi: 10.1177/1476750310362435).

Brondino, M, Pasini, M & Costa, S 2013, ‘Development and validation of an integrated organizational safety climate questionnaire with multilevel confirmatory factor analysis’, *Quality & Quantity*, vol. 47, no. 4, pp. 2191–2223 (doi: 10.1007/s11135-011-9651-6).

Brondino, M, Silva, SA & Pasini, M 2012, 'Multilevel approach to organizational and group safety climate and safety performance: co-workers as the missing link', *Safety Science*, vol. 50, no. 9, pp. 1847–1856 (doi: 10.1016/j.ssci.2012.04.010).

Brown, TA 2006, *Confirmatory factor analysis for applied research*, The Guilford Press, New York, NY.

Bruque, S, Moyano, J & Eisenberg, J 2009, 'Individual adaptation to IT-induced change: the role of social networks', *Journal of Management Information Systems*, vol. 25, no. 3, pp. 177–206 (doi: 10.2753/MIS0742-1222250305).

Bulgurcu, B, Cavusoglu, H & Benbasat, I 2010a, 'Information security policy compliance: an empirical study on rationality-based beliefs and information security awareness', *MIS Quarterly*, vol. 34, no. 3, pp. 523–548.

Bulgurcu, B, Cavusoglu, H & Benbasat, I 2010b, 'Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: an empirical investigation', in *2010 43rd Hawaii International Conference on System Sciences*, IEEE, pp. 1–7 (doi: 10.1109/HICSS.2010.312).

Burnkrant, RE & Cousineau, A 1975, 'Informational and normative social influence in buyer behavior', *Source Journal of Consumer Research*, vol. 2, no. 3, pp. 206–215 (doi: 10.1086/208633).

Burns, A, Posey, C, Roberts, TL & Lowry, PB 2017, 'Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals', *Computers in Human Behavior*, vol. 68, pp. 190–209 (doi: http://dx.doi.org/10.1016/j.chb.2016.11.018).

Burns, LR & Wholey, DR 1993, 'Adoption and abandonment of matrix management programs: effects of organizational characteristics and interoganizational networks', *Academy of Management*, vol. 36, no. 1, pp. 106–138 (doi: 10.2307/256514).

Burt, R 1987, 'Social contagion and innovation: cohesion versus structural equivalence', *American Journal of Sociology*, vol. 92, no. 6, pp. 1287–1335.

Burt, RS 2000, 'The network structure of social capital research in organizational behavior', *Research in Organizational Behavior*, vol. 22, pp. 345–423 (doi: 10.1016/S0191-3085(00)22009-1).

Burt, RS, Kilduff, M & Tasselli, S 2013, 'Social network analysis: foundations and frontiers on advantage', *Annual Review of Psychology*, vol. 64, pp. 527–547 (doi: 10.1146/annurev-psych-113011-143828).

Butler, T, Feller, J, Pope, A, Emerson, B & Murphy, C 2008, 'Designing a core IT artefact for knowledge management systems using participatory action research in a government and a non-government organisation', *Journal of Strategic Information Systems*, vol. 17, no. 4, pp. 249–267 (doi: 10.1016/j.jsis.2007.10.002).

Butts, C 2008, 'Social network analysis with sna', *Journal of Statistical Software*, vol. 24, no. 6 (doi: 10.18637/jss.v024.i06).

Butts, CT, Hunter, DR, Morris, M, Krivitsky, PN & Almquist, Z 2014, 'Introduction to exponential-family random graph (ERG or p*) modeling with ergm', pp. 1–126. < https://cran.r-project.org/web/packages/ergm/vignettes/ergm.pdf >

Byrne, BM 2010, *Structural equation modeling with AMOS: basic concepts, applications, and programming*, Routledge, New York, NY.

Caldwell, T 2016, 'Making security awareness training work', *Computer Fraud & Security*, vol. 2016, no. 6, pp. 8–14 (doi: 10.1016/S1361-3723(15)30046-4).

Campbell, JP & Beaty, EE 1971, 'Organizational climate: its measurement and relationship to work group performance', in *Annual meeting of the American Psychological Association*, Washington, DC.

Caravita, SCS, Sijtsema, JJ, Rambaran, JA & Gini, G 2014, 'Peer influences on moral disengagement in late childhood and early adolescence', *Journal of Youth and Adolescence*, vol. 43, no. 2, pp. 193–207 (doi: 10.1007/s10964-013-9953-1).

Carpenter, MA, Li, M & Jiang, H 2012, 'Social network research in organizational contexts: a systematic review of methodological issues and choices', *Journal of Management*, vol. 38, no. 4, pp. 1328–1361.

Cartwright, D & Harary, F 1956, 'Structural balance: a generalization of Heider's theory', *Psychological Review*, vol. 63, no. 5, pp. 277–293 (doi: 10.1037/h0046049).

Chan, M, Woon, I & Kankanhalli, A 2005, 'Perceptions of information security at the workplace: linking information security climate to compliant behavior', in *Perceptions of Information Privacy and Security*, vol. 1, no. 3, pp. 18–41.

Checkland, P 1991, 'From framework through experience to learning: the essential nature of action research', in HE Nissen, HK Klein and R Hirschheim (eds), *Information system research: contemporary approaches and emergent traditions*, North-Holland, Amsterdam, pp. 397–403.

Checkland, PB 1988, 'Information systems and systems thinking: time to unite?', *International Journal of Information Management*, vol. 8, no. 4, pp. 239–248 (doi: 10.1016/0268-4012(88)90031-X).

Checkland, P & Holwell, S 1998, 'Action research: its nature and validity', *Systemic Practice and Action Research*, vol. 11, no. 1, pp. 9–21 (doi: 10.1023/A:1022908820784).

Cheng, L, Li, Y, Li, W, Holm, E & Zhai, Q 2013, 'Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory', *Computers & Security*, vol. 39, pp. 447–459.

Chew, E, Swanson, M, Stine, K, Bartol, N, Brown, A & Robinson, W 2008, *Performance measurement guide for information security*, NIST Special Publication 800–55 Revision 1, U.S. Department of Commerce, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf> (doi: 10.6028/NIST.SP.800-55r1).

Chia, PA, Maynard, SB & Ruighaver, AB 2002 'Understanding Organizational Security Culture', in *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2002)*, Tokyo, Japan, pp. 1–23.

Chipperfield, C & Furnell, S 2010, 'From security policy to practice: sending the right messages', *Computer Fraud and Security*, vol. 2010, no. 3, pp. 13–19 (doi: 10.1016/S1361-3723(10)70025-7).

Cho, Y, Wang, J & Lee, D 2012, 'Identification of effective opinion leaders in the diffusion of technological innovation: a social network approach', *Technological Forecasting and Social Change*, vol. 79, no. 1, pp. 97–106 (doi: 10.1016/j.techfore.2011.06.003).

Chrusciel, D 2008, 'What motivates the significant/strategic change champion(s)?', *Journal of Organizational Change Management*, vol. 21, no. 2, pp. 148–160 (doi: 10.1108/09534810810856408).

Cialdini, RB & Goldstein, NJ 2004 'Social influence: compliance and conformity', *Annual Review of psychology*, vol. 55, no. 1974, pp. 591–621 (doi: 10.1146/annurev.psych.55.090902.142015).

Cisco 2017, *2017 Annual cybersecurity report*, viewed 14 November 2017, <https://www.cdwg.com/content/dam/CDW/resources/brands/Cisco/2017-Annual-Cybersecurity-Report.pdf>.

Clarke, S 2006, 'The relationship between safety climate and safety performance: a meta-analytic review', *Journal of Occupational Health Psychology*, vol. 11, no. 4, pp. 315–327 (doi: 10.1037/1076-8998.11.4.315).

Cole, R, Purao, S, Rossi, M & Sein, MK 2005, 'Being proactive: where action research meets design research', in *ICIS 2005 Proceedings*, pp. 1–21, <http://aisel.aisnet.org/icis2005/27>.

Cone, BD, Irvine, CE, Thompson, MF & Nguyen, TD 2007, 'A video game for cyber security training and awareness', *Computers & Security*, vol. 26, no. 1, pp. 63–72 (doi: 10.1016/j.cose.2006.10.005).

Constantine, C 2014, 'Big data: an information security context', *Network Security*, vol. 2014, no. 1, pp. 18–19 (doi: http://dx.doi.org/10.1016/S1353-4858(14)70010-8).

Corbin, J & Strauss, A 1990, 'Grounded theory research: procedures, canons, and evaluative criteria', *Qualitative Sociology*, vol. 13, no. 1, pp. 3–21.

Corona, CO 2008, *Information security awareness: an innovation approach*, Royal Holloway, University of London, <http://digirep.rhul.ac.uk/items/9e7de7b8-d65c-dc5c-222c-e33946e5d74e/1/>.

Coughlan, P & Coughlan, D 2002, 'Action research for operations management', *International Journal of Operations & Production Management*, vol. 22, no. 2, pp. 220–240.

Cross, R, Borgatti, SP & Parker, A 2002, 'Making invisible work visible: using social network analysis to support strategic collaboration', *California Management Review*, vol. 44, no. 2, pp. 25–46.

Cross, R, Laseter, T, Parker, A & Guillermo, V 2006, 'Using social network analysis to improve communities of practice', *California Management Review*, vol. 49, no. 1, pp. 32–62.

Cross, R, Laseter, T, Parker, A & Velasquez, G 2004, *Assessing and improving communities of practice with organizational network analysis*, The Network Roundtable at the University of Virginia, viewed 14 November 2017, <https://pdfs.semanticscholar.org/b3a8/6926d94a4d8e3f4213c97d64b47b90b728c8.pdf >.

Cross, R, Parker, A & Borgatti, SP 2002, 'A bird's-eye view: using social network analysis to improve knowledge creation and sharing', in IBM (ed), *IBM Institute for Business Value*, vol. 2, New York, NY, pp. 1–17 (doi: 10.2307/1315064).

Crossler, RE, Johnston, AC, Lowry, PB, Hu, Q, Warkentin, M & Baskerville, RL 2013, 'Future directions for behavioral information security research', *Computers & Security*, vol. 32, pp. 90–101 (doi: http://dx.doi.org/10.1016/j.cose.2012.09.010).

Crossler, RE, Long, JH, Loraas, TM & Trinkle, BS 2014, 'Understanding compliance with bring your own device policies utilizing protection motivation theory bridging the intention-behavior gap', *Journal of Information Systems*, vol. 28, no. 1, pp. 209–226 (doi: 10.2308/isys-50704).

Crossley, N, Bellotti, E, Edwards, G, Everett, MG, Koskinen, J & Tranmer, M 2015, *Social network analysis for ego-nets: social network analysis for actor-centred networks*, SAGE Publications.

Curley, KF & Gremillion, LL 1983, 'The role of the champion in DSS implementation', *Information and Management*, vol. 6, no. 4, pp. 203–209 (doi: 10.1016/0378-7206(83)90007-1).

D'Arcy, J & Devaraj, S 2012, 'Employee misuse of information technology resources: testing a contemporary deterrence model', *Decision Sciences*, vol. 43, no. 6, pp. 1091–1124.

D'Arcy, J & Herath, T 2011, 'A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings', *European Journal of Information Systems*, vol. 20, no. 6, pp. 643–658 (doi: 10.1057/ejis.2011.23).

D'Arcy, J & Hovav, A 2008, 'Does one size fit all? Examining the differential effects of IS security countermeasures', *Journal of Business Ethics*, vol. 89, pp. 59–71.

D'Arcy, J, Hovav, A & Galletta, D 2009, 'User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach', *Information Systems Research*, vol. 20, no. 1, pp. 79–98 (doi: 10.1287/isre.1070.0160).

Dang-Pham, D & Pittayachawan, S 2015, 'Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach', *Computers and Security*, vol. 48, pp. 281–297 (doi: 10.1016/j.cose.2014.11.002).

Dang-Pham, D, Pittayachawan, S & Bruno, V 2015, 'Factors of people-centric security climate: conceptual model and exploratory study in Vietnam', in *Proceedings of the Australasian Conference on Information Systems (ACIS 2015)*, University of South Australia, Adelaide, SA, pp. 1–14.

Davison, RM 2010, 'Retrospect and prospect: information systems in the last and next 25 years: response and extension', *Journal of Information Technology*, vol. 25, no. 4, pp. 352–354 (doi: 10.1057/jit.2010.35).

Davison, RM, Martinsons, MG & Kock, N 2004, 'Principles of canonical action research', *Information Systems Journal*, vol. 14, no. 1, pp. 65–86 (doi: 10.1111/j.1365-2575.2004.00162.x).

Davison, RM, Martinsons, MG & Ou, CXJ 2012, 'The roles of theory in canonical action research', *MIS Quarterly*, vol. 36, no. 3, pp. 763–786.

Deci, E & Eghrari, H 1994, 'Facilitating internalization: the self-determination theory perspective', *Journal of Personality*, vol. 62, no. 1, pp. 119–142.

DeLay, D, Zhang, L, Hanish, LD, Miller, CF, Fabes, RA, Martin, CL, Kochel, KP & Updegraff, KA 2016, 'Peer influence on academic performance: a social network analysis of social-emotional intervention effects', *Prevention Science*, vol. 17, no. 8, pp. 903–913 (doi: 10.1007/s11121-016-0678-8).

Denison, DR 1996, 'What is the difference between organizational culture and organizational climate? A native's point of view on a decade of paradigm wars', *Academy of Management Review*, vol. 21, no. 3, pp. 619–654.

Desmarais, BA & Cranmer, SJ 2012, 'Statistical inference for valued-edge networks: the generalized exponential random graph model', *PLoS ONE*, vol. 7, no. 1 (doi: 10.1371/journal.pone.0030136).

Detert, JR, Schroeder, RG & Mauriel, JJ 2000, 'A framework for linking culture and in improvement initiatives in organization', *Academy of Management Review*, vol. 25, no. 4, pp. 850–863 (doi: https://doi.org/10.5465/AMR.2000.3707740).

Dhillon, G & Backhouse, J 2001, 'Current directions in IS security research: towards socio-organizational perspectives', *Information Systems Journal*, vol. 11, no. 2, pp. 127–153 (doi: 10.1046/j.1365-2575.2001.00099.x).

Dhillon, G & Torkzadeh, G 2006, 'Value-focused assessment of information systems security in organizations', *Information Systems Journal*, vol. 16, no. 3, pp. 293–314 (doi: 10.1111/j.1365-2575.2006.00219.x).

Dijkstra, JK, Lindenberg, S, Veenstra, R, Steglich, C, Isaacs, J, Card, NA & Hodges, EVE 2010, 'Influence and selection processes in weapon carrying during adolescence: the roles of status, aggression, and vulnerability', *Criminology*, vol. 48, no. 1, pp. 187–220 (doi: 10.1111/j.1745-9125.2010.00183.x).

Dinev, T, Goo, J, Hu, Q & Nam, K 2009, 'User behaviour towards protective information technologies: the role of national cultural differences', *Information Systems Journal*, vol. 19, no. 4, pp. 391–412 (doi: 10.1111/j.1365-2575.2007.00289.x).

Doherty, NF & Fulford, H 2005, 'Do information security policies reduce the incidence of security breaches: an exploratory analysis', *Information Resources Management Journal*, vol. 18, no. 4, pp. 21–39.

Dourish, P & Anderson, K 2006, 'Collective information practice: exploring Privacy and security as social and cultural phenomena', *Human–Computer Interaction*, vol. 21, no. 3, pp. 319–342.

Dourish, P, Grinter, RE, de la Flor, JD & Joseph, M 2004, 'Security in the wild: user strategies for managing security as an everyday, practical problem', *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 391–401.

Dubé, L & Paré, G 2003, 'Rigor in information systems positivist case research: current practices, trends, and recommendations', *MIS Quarterly*, vol. 27, no. 4, pp. 597–635.

Eisenhardt, KM 1989, 'Building theories from case study research', *The Academy of Management Review*, vol. 14, no. 4, p. 532–550 (doi: 10.2307/258557).

Emery, C, Daniloski, K & Hamby, A 2010, 'The reciprocal effects of self-view as a leader and leadership emergence', *Small Group Research*, vol. 42, no. 2, pp. 199–224 (doi: 10.1177/1046496410389494).

Everett, C 2010, 'Embedding security: when technology is no longer enough', *Computer Fraud and Security*, vol. 2010, no. 11, pp. 5–7 (doi: 10.1016/S1361-3723(10)70143-3).

Everett, C 2015, 'Big data—the future of cyber-security or its latest threat?', *Computer Fraud & Security*, vol. 2015, no. 9, pp. 14–17 (doi: http://dx.doi.org/10.1016/S1361-3723(15)30085-3).

EY 2017, *EY's 19th global information security survey 2016–17*, viewed 14 November 2017, <http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/%24FILE/GISS_2016_Report_Final.pdf>.

Filkins, B 2016, *IT security spending trends*, SANS Institute InfoSec Reading Room, viewed 14 November 2017, <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>.

Fleming, L & Waguespack, DM 2007, 'Brokerage, boundary spanning, and leadership in open innovation communities', *Organization Science*, vol. 18, no. 2, pp. 165–180 (doi: 10.1287/orsc.1060.0242).

Flin, R, Burns, C, Mearns, K, Yule, S & Robertson, E 2006, 'Measuring safety climate in healthcare', *BMJ Quality & Safety*, vol. 15, no. 2, pp. 109–115 (doi: 10.1136/qshc.2005.014761).

Flin, R, Mearns, K, O'Connor, P & Bryden, R 2000, 'Measuring safety climate: identifying the common features', *Safety Science*, vol. 34, no. 1–3, pp. 177–192.

Foltz, CB, Schwager, PH & Anderson, JE 2008, 'Why users (fail to) read computer usage policies', *Industrial Management & Data Systems*, vol. 108, no. 6, pp. 701–712 (doi: 10.1108/02635570810883969).

Fombrun, CJ 1982, 'Strategies for network research in organizations', *The Academy of Management Review*, vol. 7, no. 2, pp. 280–291.

Foorthuis, R & Brinkkemper, S 2008, 'Best practices for business and systems analysis in projects conforming to enterprise architecture', *Enterprise Modelling and Information Systems Architectures*, vol. 3, no. 1, pp. 36–47.

Forehand, GA & von Haller, G 1964, 'Environmental variation in studies of organizational behavior', *Psychological Bulletin*, vol. 62, no. 6, pp. 361–382.

Fortuin, J, van Geel, M & Vedder, P 2015, 'Peer influences on internalizing and externalizing problems among adolescents: a longitudinal social network analysis', *Journal of Youth and Adolescence*, vol. 44, no. 4, pp. 887–897 (doi: 10.1007/s10964-014-0168-x).

Fosnot, CT & Perry, RS 2005, 'Constructivism: a psychological theory of learning', in CT Fosnot (ed), *Constructivism: theory, perspectives, and practice*, 2nd edn, Teachers College Press, New York, NY, pp. 8–38.

Frank, H, Norman, RZ & Cartwright, D 1965, *Structural models: an introduction to the theory of directed graphs*, Wiley, New York, NY.

Freeman, L 2004, *The development of social network analysis: a study in the sociology of science*, Empirical Press Vancouver, BC, Canada.

French, JRP & Raven, B 1959, 'The bases of social power', in D Cartwright (ed), *Studies in social power*, University of Michigan, Oxford, UK, pp. 150–167.

Fuerstenau, D & Rothe, H 2014, 'Shadow IT systems: discerning the good and the evil', in *ECIS 2014 Proceedings*, pp. 0–14, <http://aisel.aisnet.org/ecis2014/proceedings/track15/9/>

Furnell, S & Rajendran, A 2012, 'Understanding the influences on information security behaviour', *Computer Fraud and Security*, vol. 2012, no. 3, pp. 12–15 (doi: 10.1016/S1361-3723(12)70053-2).

Furnell, S & Thomson, KL 2009, 'From culture to disobedience: recognising the varying user acceptance of IT security', *Computer Fraud and Security*, vol. 2009, no. 2, pp. 5–10 (doi: 10.1016/S1361-3723(09)70019-3).

Furstenau, D, Rothe, H, Sandner, M & Anapliotis, D 2016, 'Shadow IT, risk, and shifting power relations in organizations', in *AMCIS 2016 Proceedings*, pp. 1–10.

Gabriel, T & Furnell, S 2011, 'Selecting security champions', *Computer Fraud and Security*, vol. 2011, no. 8, pp. 8–12 (doi: 10.1016/S1361-3723(11)70082-3).

Gagné, M & Deci, EL 2005, 'Self-determination theory and work motivation', *Journal of Organizational Behavior*, vol. 26, no. 4, pp. 331–362.

Gallivan, MJ, Spitler, VK & Koufaris, M 2005, 'Does information technology training really matter? A social information processing analysis of coworkers' influence on IT usage in the workplace', *Journal of Management Information Systems*, vol. 22, no. 1, pp. 153–192.

Gaunt, N 2000, 'Practical approaches to creating a security culture', *International Journal of Medical Informatics*, vol. 60, no. 2, pp. 151–157, <http://www.ncbi.nlm.nih.gov/pubmed/11154966>.

Gerber, M & von Solms, R 2005, 'Management of risk in the information age', *Computers and Security*, vol. 24, no. 1, pp. 16–30 (doi: 10.1016/j.cose.2004.11.002).

Gerring, J 2004, 'What is a case study and what is it good for?', *American Political Science Review*, vol. 98, no. 2, pp. 341–354.

Gesell, SB, Barkin, SL & Valente, TW 2013, 'Social network diagnostics: a tool for monitoring group interventions', *Implementation Science*, vol. 8, no. 1, Implementation Science, p. 116 (doi: 10.1186/1748-5908-8-116).

Gibson, CB 2001, 'From knowledge accumulation to accommodation: cycles of collective cognition in work groups', *Journal of Organizational Behavior*, vol. 22, no. 2, pp. 121–134 (doi: 10.1002/job.84).

Gikas, C 2010, 'A general comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS standards', *Information Security Journal: A Global Perspective*, vol. 19, no. 3, pp. 132–141 (doi: 10.1080/19393551003657019).

Glisson, C 2007, 'Assessing and changing organizational culture and climate for effective services', *Research on Social Work Practice*, vol. 17, vol. 6, pp. 736–747 (doi: https://doi.org/10.1177/1049731507301659).

Goldkuhl, G 2011, 'The research practice of practice research: theorizing and situational inquiry', *Systems, Signs & Actions*, vol. 5, no. 1, pp. 7–29.

Goldkuhl, G 2012a, 'From action research to practice research', *Australasian Journal of Information Systems*, vol. 17, no. 2, pp. 57–78 (doi: 10.3127/ajis.v17i2.688).

Goldkuhl, G 2012b, 'Pragmatism vs interpretivism in qualitative information systems research', *European Journal of Information Systems*, vol. 21, no. 2, pp. 135–146 (doi: 10.1057/ejis.2011.54).

Goo, J, Yim, M & Kim, D 2014, 'A path to successful management of employee security compliance: an empirical study of information security climate', *IEEE Transactions on Professional Communication*, vol. 57, no. 4, pp. 1–24.

Goodhue, DL & Straub, DW 1991, 'Security concerns of system users', *Information & Management*, vol. 20, no. 1, pp. 13–27 (doi: 10.1016/0378-7206(91)90024-V).

Goodreau, SM, Handcock, MS, Hunter, DR, Butts, CT & Morris, M 2008, 'A statnet tutorial', *Journal of Statistical Software*, vol. 24, no. 9, pp. 1–27 (doi: 10.1016/j.biotechadv.2011.08.021.Secreted).

Gould, RRV 1993, ‘Collective action and network structure’, *American Sociological Review*, vol. 58, no. 2, pp. 182–196.

Gould, RV & Fernandez, RM 1989, ‘Structures of mediation: a formal approach to brokerage in transaction networks’, *Sociological Methodology*, vol. 19, no. 1989, pp. 89–126.

Graham, JM 2006, ‘Congeneric and (essentially) tau-equivalent estimates of score reliability. What they are and how to use them’, *Educational and Psychological Measurement*, vol. 66, no. 6, pp. 930–944.

Greenhalgh, T, Robert, G, Macfarlane, F, Bate, P & Kyriakidou, O 2004, ‘Diffusion of innovations in service organizations: systematic review and recommendations’, *Milbank Quarterly*, vol. 82, no. 4, pp. 581–629 (doi: 10.1111/j.0887-378X.2004.00325.x).

Greenwood, DJ & Levin, M 2007, *Introduction to action research: social research for social change*, 2nd edn, SAGE Publications.

Guion, R 1973, ‘A note on organizational climate’, *Organizational Behavior and Human Performance*, vol. 9, no. 1, pp. 120–125.

Guldenmund, F 2000, ‘The nature of safety culture: a review of theory and research’, *Safety Science*, vol. 34, no. 1, pp. 215–257 (doi: 10.1016/S0925-7535(00)00014-X).

Guo, KH 2013, ‘Security-related behavior in using information systems in the workplace: a review and synthesis’, *Computers & Security*, vol. 32, no. 1, pp. 242–251 (doi: 10.1016/j.cose.2012.10.003).

Guo, KH & Yuan, Y 2012, ‘The effects of multilevel sanctions on information security violations: a mediating model’, *Information & Management*, vol. 49, no. 6, pp. 320–326 (doi: http://dx.doi.org/10.1016/j.im.2012.08.001).

Guo, KH, Yuan, Y, Archer, NP & Connelly, CE 2011, ‘Understanding nonmalicious security violations in the workplace: a composite behavior model’, *Journal of Management Information Systems*, vol. 28, no. 2, pp. 203–236 (doi: 10.2753/MIS0742-1222280208).

Guttman, B & Roback, EA 1995, *An introduction to computer security: the NIST handbook*, NIST Special Publication 800-12, U.S. Department of Commerce, viewed 5 June 2016, <https://csrc.nist.gov/publications/detail/sp/800-12/archive/1995-10-02>.

Halgin, DS & Borgatti, SP 2012, 'An introduction to personal network analysis and tie churn statistics using E-NET', *Connections*, vol. 32, pp. 37–48.

Hancock, GR & Mueller, RO 2001, 'Rethinking construct reliability within latent variable systems', in R Cudeck, S Du Toit and D Söbom (eds) *Structural equation modeling: present and future*, Scientific Software International, Lincolnwood, IL, pp. 195–216.

Hanneman, RA & Riddle, M 2005, *Introduction to social network methods*, University of California, Riverside, CA.

Hansen, B 2009, 'Beyond the process: enriching software process improvement with knowledge management', PhD Thesis, Copenhagen Business School, Frederiksberg <http://openarchive.cbs.dk/handle/10398/7902?show=full>.

Hanus, B & Wu, Y 2016, 'Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective', *Information Systems Management*, vol. 33, no. 1, pp. 2–16 (doi: 10.1080/10580530.2015.1117842).

Harrington, S 1996, 'The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions', *MIS Quarterly*, vol. 20, no. 3, pp. 257–278.

Harris, J, Ives, B & Junglas, I 2011, 'IT consumerization: when gadgets turn into enterprise IT tools', *MIS Quarterly Executive*, vol. 10, no. 2, pp. 115–117.

Hatala, J-P 2006, 'Social network analysis in human resource development: a new methodology', *Human Resource Development Review*, vol. 5, no. 1, pp. 45–71 (doi: 10.1177/1534484305284318).

Hatala, J-P & Fleming, PR 2007, 'Making transfer climate visible: utilizing social network analysis to facilitate the transfer of training', *Human Resource Development Review*, vol. 6, no. 1, pp. 33–63 (doi: 10.1177/1534484306297116).

Hatala, J-P & Lutta, JG 2009, 'Managing information sharing within an organizational setting: a social network perspective', *Performance Improvement Quarterly*, vol. 21, no. 4, pp. 5–33.

Hawkins, S, Yen, DC & Chou, DC 2000, 'Awareness and challenges of internet security', *Information Management & Computer Security*, vol. 8, no. 3, pp. 131–143.

Heikka, J 2008, 'A constructive approach to information systems security training: an action research experience', in *14th Americas Conference on Information Systems, AMCIS 2008*, vol. 1, pp. 15–22, <http://www.scopus.com/inward/record.url?eid=2-s2.0-84870358273&partnerID=40&md5=15da3b6a475b1e8f9c511f587e9bc2a9>.

Heikkinen, HLT, Huttunen, R, Syrjälä, L & Pesonen, J 2012, 'Action research and narrative inquiry: five principles for validation revisited', *Educational Action Research*, vol. 20, no. 1, pp. 5–21 (doi: 10.1080/09650792.2012.647635).

Herath, T & Rao, HR 2009a, 'Protection motivation and deterrence: a framework for security policy compliance in organisations', *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–125.

Herath, T & Rao, HR 2009b, 'Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness', *Decision Support Systems*, vol. 47, no. 2, pp. 154–165 (doi: http://dx.doi.org/10.1016/j.dss.2009.02.005).

Hirschi, T 1969, *Causes of delinquency*, University of California, Berkeley, CA.

Hofstede, G 2001, *Culture's consequences: comparing values, behaviors, institutions, and organizations across nations*, 2nd edn, SAGE Publications, Thousand Oaks, CA.

Holland, P & Leinhardt, S 1976, 'Local structure in social networks', *Sociological Methodology*, vol. 7, no. 1976, pp. 1–45 (doi: 10.2307/270703).

Holmberg, L, Nilsson, A, Olsson, HH & Sandberg, AB 2009, 'Appreciative inquiry in software process improvement', *Software Process: Improvement and Practice*, vol. 14, no. 2, pp. 107–125 (doi: 10.1002/spip.407).

Höne, K & Eloff, JHP 2002, 'What makes an effective information security policy?', *Network Security*, vol. 2002, no. 6, pp. 14–16 (doi: http://dx.doi.org/10.1016/S1353-4858(02)06011-7).

Hornik, K 2016, *R FAQ. Frequently asked questions on R*, viewed 5 Jun 2017, <https://cran.r-project.org/doc/FAQ/R-FAQ.html>.

Hovav, A & D'Arcy, J 2012, 'Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea', *Information & Management*, vol. 49, no. 2, pp. 99–110 (doi: http://dx.doi.org/10.1016/j.im.2011.12.005).

Howell, JM & Boies, K 2004, 'Champions of technological innovation: the influence of contextual knowledge, role orientation, idea generation, and idea promotion on champion emergence', *Leadership Quarterly*, vol. 15, no. 1, pp. 123–143 (doi: 10.1016/j.leaqua.2003.12.008).

Howell, JM & Higgins, CA 1990, 'Leadership behaviors, influence tactics and career experiences of champions of technological innovation', *The Leadership Quarterly*, vol. 1, no. 4, pp. 249–264 (doi: http://dx.doi.org/10.1016/1048-9843(90)90004-2).

Hu, Q, Dinev, T, Hart, P & Cooke, D 2012, 'Managing employee compliance with information security policies: the critical role of top management and organizational culture', *Decision Sciences*, vol. 43, no. 4, pp. 615–660 (doi: 10.1111/j.1540-5915.2012.00361.x).

Hu, Q, Xu, Z, Dinev, T & Ling, H 2011, 'Does deterrence work in reducing information security policy abuse by employees?', *Communications of the ACM*, vol. 54, no. 6, p. 54.

Huang, J & Martin-Taylor, M 2013, 'Turnaround user acceptance in the context of HR self-service technology adoption: an action research approach', *International Journal of Human Resource Management*, vol. 24, no. 3, pp. 621–642 (doi: 10.1080/09585192.2012.677460).

Huang, S-M, Lee, C-L & Kao, A-C 2006, 'Balancing performance measures for information security management: a balanced scorecard framework', *Industrial Management & Data Systems*, vol. 106, no. 2, pp. 242–255 (doi: 10.1108/02635570610649880).

Hult, M & Lennung, S-Å 1980, 'Towards a definition of action research: a note and a bibliography', *Journal of Management Studies*, vol. 17, no. 2, pp. 241–250 (doi: 10.1111/j.1467-6486.1980.tb00087.x).

Humaidi, N & Balakrishnan, V 2015, 'Leadership styles and information security compliance behavior: the mediator effect of information security awareness', *International Journal of Information and Education Technology*, vol. 5, no. 4, pp. 311–318 (doi: 10.7763/IJIET.2015.V5.522).

Hunter, DR, Handcock, MS, Butts, CT, Goodreau, SM & Morris, M 2008, 'ergm: a package to fit, simulate and diagnose exponential-family models for networks', *Journal of Statistical Software*, vol. 24, no. 3 (doi: 10.18637/jss.v024.i03).

Ibarra, H 1993, 'Network centrality, power, and innovation involvement: determinants of technical and administrative roles', *The Academy of Management Journal*, vol. 36, no. 3, pp. 471–501.

Ibarra, H & Andrews, SB 1993, 'Power, social influence, and sense making: effects of network centrality and proximity on employee perceptions', *Administrative Science Quarterly*, vol. 38, no. 2, p. 277 (doi: 10.2307/2393414).

IBM 2006, *IBM Information security framework*, viewed 14 November 2016, <https://www-935.ibm.com/services/us/igs/pdf/g510-6454-information-security-framework.pdf>.

Ifinedo, P 2012, 'Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory', *Computers and Security*, vol. 31, no. 1, pp. 83–95 (doi: 10.1016/j.cose.2011.10.007).

Ifinedo, P 2014, 'Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition', *Information and Management*, vol. 51, no. 1, pp. 69–79 (doi: 10.1016/j.im.2013.10.001).

Internet Live Stats 2016, *Internet users by country (2016)*, viewed 5 July 2016, <http://www.internetlivestats.com/internet-users-by-country>.

ISO 2017, *ISO/IEC 27001 family - Information security management*, viewed 5 June 2016, <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>.

Iversen, JH, Mathiassen, L & Nielsen, PA 2004, 'Managing risk in software process improvement: an action research approach', *MIS Quarterly*, vol. 28, no. 3, pp. 395–434.

Jaafar, NI & Ajis, A 2013, 'Organizational climate and individual factors effects on information security faculty of business and accountancy', *International Journal of Business and Social Science*, vol. 4, no. 10, pp. 118–130.

James, L & Jones, A 1974, 'Organizational climate: a review of theory and research', *Psychological Bulletin*, vol. 81, no. 12, pp. 1096–1112.

Jarvinen, P 2007, 'Action research is similar to design science', *Quality and Quantity*, vol. 41, no. 1, pp. 37–54 (doi: 10.1007/s11135-005-5427-1).

Jenssen, JI & Jørgensen, G 2004, 'How do corporate champions promote innovations?', *International Journal of Innovation Management*, vol. 8, no. 1, pp. 63–86 (doi: 10.1142/S1363919604000964).

Johnston, AC & Warkentin, M 2010, 'Fear appeals and information security behaviors: an empirical study', *MIS Quarterly*, vol. 34, no. 3, pp. 549–566.

Johnson-Cramer, M, Parise, S & Cross, R 2007, 'Managing change through networks and values', *California Management Review*, vol. 49, no. 3, pp. 85–109.

Kabay, M 1994, 'Psychosocial factors in the implementation of information security policy', *EDPACS: The EDP Audit, Control, and Security Newsletter*, vol. 21, no. 10, pp. 1–10 (doi: 10.1080/07366989409451659).

Kajtazi, M, Cavusoglu, H, Benbasat, I & Haftor, D 2013, 'Assessing self-justification as an antecedent of noncompliance with information security policies,' in *Australasian Conference on Information Systems (ACIS)*, Melbourne, Australia.

Kajzer, M, D'Arcy, J, Crowell, CR, Striegel, A & van Bruggen, D 2014, 'An exploratory investigation of message-person congruence in information security awareness campaigns', *Computers & Security*, vol. 43, pp. 64–76 (doi: http://dx.doi.org/10.1016/j.cose.2014.03.003).

Kane, G, Alavi, M, Labianca, G & Borgatti, SP 2014, 'What's different about social media networks? A framework and research agenda', *MIS Quarterly*, vol. 38, no. 1, pp. 1–30.

Karjalainen, M & Siponen, M 2011, 'Toward a new meta-theory for designing information systems (IS) security training approaches', *Journal of the Association for Information Systems*, vol. 12, no. 8, pp. 518–555.

Karjalainen, M, Siponen, M, Petri, P & Suprateek, S 2013, 'One size does not fit all: different cultures require different information systems security interventions', in *PACIS 2013 Proceedings*, <http://aisel.aisnet.org/pacis2013/98/>.

Karlsson, F, Åström, J & Karlsson, M 2015, 'Information security culture – state-of-the-art review between 2000 and 2013', *Information & Computer Security*, vol. 23, vol. 3, pp. 246–285 (doi: https://doi.org/https://doi.org/10.1108/ICS-05-2014-0033).

Karyda, M, Kiountouzis, E & Kokolakis, S 2005, 'Information systems security policies: a contextual perspective', *Computers & Security*, vol. 24, no. 3, pp. 246–260 (doi: 10.1016/j.cose.2004.08.011).

Kaspersky 2014, *Kaspersky Security Bulletin 2014*, viewed 14 November 2017, <https://securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014-EN.pdf>.

Kelman, HC 1961, 'Processes of opinion change', *The Public Opinion Quarterly*, vol. 25, no. 1, pp. 57–78 (doi: 10.2307/2746461).

Kim, J, Park, EH & Baskerville, RL 2016, 'A model of emotion and computer abuse', *Information and Management*, vol. 53, no. 1, pp. 91–108 (doi: 10.1016/j.im.2015.09.003).

Kim, SS & Kim, YJ 2016, 'The effect of compliance knowledge and compliance support systems on information security compliance behavior', *Journal of Knowledge Management*, vol. 21, no. 4, pp. 986–1010 (doi: 10.1108/JKM-08-2016-0353).

Kines, P, Lappalainen, J, Lyngby, K, Olsen, E, Pousette, A, Tharaldsen, J, Tómasson, K & Törner, M 2011, 'Nordic safety climate questionnaire (NOSACQ-50): a new tool for diagnosing occupational safety climate', *International Journal of Industrial Ergonomics*, vol. 41, no. 6, pp. 634–646 (doi: 10.1016/j.ergon.2011.08.004).

Kirkpatrick, DL 2006, *Evaluating training programs: the four levels*, 3rd edn, Berrett-Koehler, San Francisco, CA.

Kirlappos, I, Beautement, A & Sasse, MA 2013, ' "Comply or die" is dead: long live security-aware principal agents', in AA Adams, M Brenner and M Smith (eds), *Financial cryptography and data security*, Springer Berlin, Heidelberg, Germany, pp. 70–82.

Kirlappos, I, Parkin, S & Sasse, MA 2014, 'Learning from "shadow security": why understanding non-compliant behaviors provides the basis for effective security', in *USEC'14 Workshop on Usable Security*, NDSS San Diego, California, 23–26 February, pp. 1–10, viewed 5 June 2017, <https://www.ndss-symposium.org/ndss2014/workshop-usable-security-usec-2014-programme/learning-shadow-security-why-understanding-non-compliance-provides-basis-effective-security/>.

Kissel, R (ed) 2013, *Glossary of key information security terms*, NISTIR 7298 Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce, <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf> (doi: 10.6028/NIST.IR.7298r2).

Klein, HK & Myers, MD 1999, 'A set of principles for conducting and evaluating interpretive field studies in information systems', *MIS Quarterly*, vol. 23, no. 1, pp. 67–93.

Kline, RB 2011, *Principles and practice of structural equation modeling*, 3rd edn, Guilford Press, New York, NY.

Kolb, AY & Kolb, DA 2011, 'Experiential learning theory: a dynamic, holistic approach to management learning, education and development', in SJ Armstrong and CV Fukami (eds), *The SAGE handbook of management learning, education and development*, SAGE Publications, pp. 42–68 (doi: 10.4135/9780857021038.n3).

Kolb, DA (ed) 1984, *Experiential learning: experience as the source of learning and development*, Prentice-Hall, Englewoods Cliffs, NJ (doi: 10.1016/B978-0-7506-7223-8.50017-4).

Kotulic, AG & Clark, JG 2004, 'Why there aren't more information security research studies', *Information & Management*, vol. 41, no. 5, pp. 597–607 (doi: http://dx.doi.org/10.1016/j.im.2003.08.001).

Kraatz, MS 1998, 'Learning by association? Interorganizational networks and adaptation to environmental change', *Academy of Management Journal*, vol. 41, no. 6, pp. 621–643 (doi: 10.2307/256961).

Kraemer, S, Carayon, P & Clem, J 2009, 'Human and organizational factors in computer and information security: pathways to vulnerabilities', *Computers & Security*, vol. 28, no. 7, pp. 509–520 (doi: http://dx.doi.org/10.1016/j.cose.2009.04.006).

Krefting, L 1991, 'Rigor in qualitative research: the assesment of trustworthiness', *American Journal of Occupational Therapy*, vol. 45, no. 3, pp. 214–222.

Kuenzi, M & Schminke, M 2009, 'Assembling fragments into a lens: a review, critique, and proposed research agenda for the organizational work climate literature', *Journal of Management*, vol. 35, no. 3, pp. 634–717.

Leach, J 2003, 'Improving user security behaviour', *Computers & Security*, vol. 22, no. 8, pp. 685–692.

Lebek, B, Uffen, J, Neumann, M, Hohler, B & Breitner, MH 2014, 'Information security awareness and behavior: a theory-based literature review', *Management Research Review*, vol. 37, no. 12, pp. 1049–1092 (doi: 10.1108/MRR-04-2013-0085).

Lee, AS 2010, 'Retrospect and prospect: information systems research in the last and next 25 years', *Journal of Information Technology*, vol. 25, no. 4, pp. 336–348 (doi: 10.1057/jit.2010.24).

Lee, D, Larose, R & Rifon, N 2008, 'Keeping our network safe: a model of online protection behaviour', *Behaviour & Information Technology*, vol. 27, no. 5, pp. 445–454.

Lee, SM, Lee, S-G & Yoo, S 2004, 'An integrative model of computer abuse based on social control and general deterrence theories', *Information & Management*, vol. 41, no. 6, pp. 707–718.

Lee, Y & Kozar, KA 2008, 'An empirical investigation of anti-spyware software adoption: a multitheoretical perspective', *Information & Management*, vol. 45, no. 2, pp. 109–119 (doi: 10.1016/j.im.2008.01.002).

Leenders, RTAJ 2002, 'Modeling social influence through network autocorrelation: constructing the weight matrix', *Social Networks*, vol. 24, no. 1, pp. 21–47.

Leonard, LNK, Cronan, TP & Kreie, J 2004, 'What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics?', *Information and Management*, vol. 42, no. 1, pp. 143–158 (doi: 10.1016/j.im.2003.12.008).

Lewis, BR, Templeton, GF & Byrd, TA 2005, 'A methodology for construct development in MIS research', *European Journal of Information Systems*, vol. 14, no. 4, pp. 388–400.

Lewis, LK & Seibold, DR 1998, 'Reconceptualizing organizational change implementation as a communication problem: a review of literature and research agenda', *Annals of the International Communication Association*, vol. 21, no. 1, pp. 93–152 (doi: 10.1080/23808985.1998.11678949).

Li, H, Zhang, J & Sarathy, R 2010, 'Understanding compliance with internet use policy from the perspective of rational choice theory', *Decision Support Systems*, vol. 48, no. 4, pp. 635–645.

Liang, H & Xue, Y 2010, 'Understanding security behaviors in personal computer usage: a threat avoidance perspective', *Journal of the Association for Information Systems*, vol. 11, no. 7, pp. 394–413.

Lich, N 2016, *Vietnam's information security index upgraded, but high risks exist*, VietNamNet Bridge, viewed 14 November 2017, <http://english.vietnamnet.vn/fms/science-it/168016/vietnam-s-information-security-index-upgraded--but-high-risks-exist.html>.

Lindgren, R, Henfridsson, O & Schultze, U 2004, 'Design principles for competence management systems: a synthesis of an action research study', *MIS Quarterly*, vol. 28, no. 3, pp. 435–472.

Lingard, HC, Cooke, T & Blismas, N 2009, 'Group-level safety climate in the Australian construction industry: within-group homogeneity and between-group differences in road construction and maintenance', *Construction Management and Economics*, vol. 27, no. 4, pp. 419–432 (doi: 10.1080/01446190902822971).

Liu, W, Sidhu, A, Beacom, AM & Valente, TW 2017, 'Social network theory', in P Rössler (ed), *The International Encyclopedia of Media Effects*, Wiley, pp. 1–12 (doi: 10.1002/9781118783764.wbieme0092).

Loch, KD, Carr, HH & Warkentin, ME 1992, 'Threats to information systems: today's reality, yesterday's understanding', *MIS Quarterly*, vol. 16, no. 2, pp. 173–186.

Loch, KDD & Carr, HHH 1991, 'Threats to information system security: an organizational perspective', in *Proceedings of the Twenty-Fourth Annual Hawaii International Conference on System Sciences, 1991*, vol. 4, 8–11 January, pp. 551–557 (doi: 10.1109/HICSS.1991.184104).

Lomi, A, Snijders, TAB, Steglich, CEG & Torlo, VJ 2011, 'Why are some more peer than others? Evidence from a longitudinal study of social networks and individual academic performance', *Social Science Research*, vol. 40, no. 6, pp. 1506–1520 (doi: 10.1016/j.ssresearch.2011.06.010).

Lowry, PB & Moody, GD 2013, 'Explaining opposing compliance motivations towards organizational information security policies', *2013 46th Hawaii International Conference on System Sciences*, IEEE, pp. 2998–3007 (doi: 10.1109/HICSS.2013.5).

Lowry, PB & Moody, GD 2015, 'Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies', *Information Systems Journal*, vol. 25, no. 5, pp. 433–463 (doi: 10.1111/isj.12043).

Luce, RD & Perry, AD 1949, 'A method of matrix analysis of group structure', *Psychometrika*, vol. 14, no. 2, pp. 95–116 (doi: 10.1007/BF02289146).

Lusher, D, Koskinen, J & Robins, G 2012, *Exponential random graph models for social networks: theory, methods, and applications*, Cambridge University Press.

Ma, Q, Johnston, AC & Pearson, JM 2008, 'Information security management objectives and practices: a parsimonious framework', *Information Management & Computer Security*, vol. 16, no. 3, pp. 251–270 (doi: 10.1108/09685220810893207).

Malaurent, J & Avison, D 2016, 'Reconciling global and local needs: a canonical action research project to deal with workarounds', *Information Systems Journal*, vol. 26, no. 3, pp. 227–257 (doi: 10.1111/isj.12074).

Malliaros, FD & Vazirgiannis, M 2013, 'Clustering and community detection in directed networks: a survey', *Physics Reports*, vol. 533, no. 4, pp. 95–142 (doi: 10.1016/j.physrep.2013.08.002).

Markus, ML & Mao, J-Y 2004, 'Participation in development and implementation - updating an old, tired concept for today's IS', *Journal of the Association for Information Systems*, vol. 5, no. 11, pp. 514–544 (doi: 10.1097/01.jcp.0000227700.26375.39).

Martinez-Moyano, IJ, Samsa, ME, Burke, JF & Akcam, BK 2008, 'Toward a generic model of security in an organizational context: exploring insider threats to information infrastructure', in *Proceedings of the 41st Hawaii International Conference on System Sciences*, 7–10 Jan, IEEE, pp. 267–276 (doi: http://doi.ieeecomputersociety.org/10.1109/HICSS.2008.456).

Martinsons, MG 1993, 'Cultivating the champions for strategic information systems', *Journal of Systems Management*, vol. 44, no. 8, pp. 31–38.

Mathiassen, L 2002, 'Collaborative practice research', *Information Technology & People*, vol. 15, no. 4, pp. 321–345 (doi: 10.1108/09593840210453115).

Mathiassen, L & Sandberg, A 2013, 'How a professionally qualified doctoral student bridged the practice-research gap: a confessional account of collaborative practice research', *European Journal of Information Systems*, vol. 22, no. 4, pp. 475–492 (doi: 10.1057/ejis.2012.35).

McCormac, A, Zwaans, T, Parsons, K, Calic, D, Butavicius, M & Pattinson, M 2016, 'Individual differences and information security awareness', *Computers in Human Behavior*, vol. 69, pp. 151–156 (doi: http://dx.doi.org/10.1016/j.chb.2016.11.065).

McKay, J & Marshall, P 2001, 'The dual imperatives of action research', *Information Technology & People*, vol. 14, no. 1, pp. 46–59 (doi: 10.1108/09593840110384771).

McKnight, DH 2002, 'Developing and validating trust measures for e-commerce: an integrative typology', *Information Systems Research*, vol. 13, no. 3, pp. 334–359 (doi: 10.1287/isre.13.3.334.81).

McPherson, M, Smith-Lovin, L & Cook, JM 2001, 'Birds of a feather: homophily in social networks', *Annual Review of Sociology*, vol. 27, no. 2001, pp. 415–444 (doi: 10.1146/annurev.soc.27.1.415).

Merete, HJ, Albrechtsen, E & Hovden, J 2008, 'Implementation and effectiveness of organizational information security measures', *Information Management & Computer Security*, vol. 16, no. 4, pp. 377–397 (doi: 10.1108/09685220810908796).

Merluzzi, J & Burt, RS 2013, 'How many names are enough? Identifying network effects with the least set of listed contacts', *Social Networks*, vol. 35, no. 3, pp. 331–337 (doi: 10.1016/j.socnet.2013.03.004).

Miller, J 2007, *The holistic curriculum*, 2nd edn, OISE Press, Toronto, Canada.

Miller, KW, Voas, J & Hurlburt, GF 2012, 'BYOD: security and privacy considerations', *IT Professional*, pp. 53–55.

Mitchell, JC 1969, 'The concept and use of social networks', in JC Mitchell (ed), *Social networks in urban situations*, Manchester University Press, UK.

Moe, NB, Dingsøyr, T, Nilsen, KR & Villmones, NJ 2005, 'Project web and electronic process guide as software process improvement', in *EuroSPI 2005, LNCS 3792*, Springer-Verlag Berlin Heidelberg, pp. 175–186.

Mohamed, N & Ahmad, IH 2012, 'Information privacy concerns, antecedents and privacy measure use in social networking sites: evidence from Malaysia', *Computers in Human Behavior*, vol. 28, no. 6, pp. 2366–2375.

Moran, ET & Wolkwein, JF 1992, 'The cultural approach to the formation of organizational climate', *Human Relations*, vol. 45, no. 1, pp. 19–47.

Moreno, JL 1934, *Who shall survive? A new approach to the problems of human interrelations*, Nervous and Mental Disease Publishing Co., Washington, DC.

Morris, M, Handcock, MS & Hunter, DR 2008, 'Specification of exponential-family random graph models: terms and computational aspects', *Journal of Statistical Software*, vol. 24, no. 4, pp. 1548–7660.

Morrison, EW 1993, 'Newcomer information seeking: exploring types, modes, sources, and outcomes', *Academy of Management Journal*, vol. 36, no. 3, pp. 557–589.

Mouw, T 2006, 'Estimating the causal effect of social capital: a review of recent research', *Annual Review of Sociology*, vol. 32, no. 1, pp. 79–102 (doi: 10.1146/annurev.soc.32.061604.123150).

Müller-Prothmann, T 2007, 'Social network analysis: a practical method to improve knowledge sharing', in AS Kazi, L Wohlfahrt and P Wolf (eds), *Hands-on knowledge co-creation and sharing; practical methods and techniques*, Knowledge Board, Stuttgart, Germany, pp. 219–233 (doi: 10.2139/ssrn.1467609).

Mumford, E 1995, *Effective systems design and requirements analysis: the ETHICS approach*, Palgrave Macmillan.

Murphy, E 1997, *Constructivism: from philosophy to practice*, viewed 5 June 2017, <https://files.eric.ed.gov/fulltext/ED444966.pdf>.

Myyry, L, Siponen, M, Pahnila, S, Vartiainen, T & Vance, A 2009, 'What levels of moral reasoning and values explain adherence to information security rules? An empirical study', *European Journal of Information Systems*, vol. 18, no. 2, pp. 126–139 (doi: 10.1057/ejis.2009.10).

Nelson, RE 1988, 'Social network analysis as an intervention tool', *Group & Organization Studies*, vol. 13, no. 1, pp. 39–58.

Ng, B-Y, Kankanhalli, A & Xu, Y 2009, 'Studying users' computer security behavior: a health belief perspective', *Decision Support Systems*, vol. 46, no. 4, pp. 815–825.

Niehaves, B, Köffer, S & Ortbach, K 2012, 'IT consumerization—a theory and practice review', in *Proceedings of 18th Americas Conference on Information Systems (AMCIS)*, vol. 1, pp. 4705–4713.

van Niekerk, JF & von Solms 2010, 'Information security culture: a management perspective', *Computers & Security*, vol. 29, no. 4, pp. 476–486 (doi: http://dx.doi.org/10.1016/j.cose.2009.10.005).

Nielsen, PA & Tjørnehøj, G 2005, 'Mapping social networks in software process improvement: an action research study', *IFIP Advances in Information and Communication Technology*, vol. 180, no. 2004, pp. 73–90.

Nielsen, PA & Tjørnehøj, G 2010, 'Social networks in software process improvement', *Journal of Software Maintenance and Evolution: Research and Practice*, vol. 22, no. 1, pp. 33–51 (doi: 10.1002/spip.419).

NIST 2011, *Managing information security risk: organization, mission, and information system view*, NIST Special Publication 800-39, U.S. Department of Commerce, viewed 14 November 2017 <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>.

Norman, P, Boer, H, and Seydel, ER 2005. 'Protection motivation theory', in M Conner & P Nornam (eds), *Predicting Health Behaviour: Research and Practice with Social Cognition Models*. Open University Press, Maidenhead, pp. 81–126.

O'Connor, P, O'Dea, A, Kennedy, Q & Buttrey, SE 2011, 'Measuring safety climate in aviation: a review and recommendations for the future', *Safety Science*, vol. 49, no. 2, pp. 128–138 (doi: 10.1016/j.ssci.2010.10.001).

Öğütçü, G, Testik, ÖM & Chouseinoglou, O 2016, 'Analysis of personal information security behavior and awareness', *Computers & Security*, vol. 56, pp. 83–93 (doi: 10.1016/j.cose.2015.10.002).

Oquist, P 1978, 'The epistemology of action research', *Acta Sociologica*, vol. 21, no. 4, pp. 143–163 (doi: 10.1177/000169937802100404).

Otte, E & Rousseau, R 2002, 'Social network analysis: a powerful strategy, also for the information sciences', *Journal of Information Science*, vol. 28, no. 6, pp. 441–453 (doi: 10.1177/016555150202800601).

Padayachee, K 2012, 'Taxonomy of compliant information security behavior', *Computers & Security*, vol. 31, no. 5, pp. 673–680 (doi: http://dx.doi.org/10.1016/j.cose.2012.04.004).

Pahnila, S, Siponen, M & Mahmood, A 2007, 'Employees' behavior towards IS security policy compliance', in *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS 2007)*, 3–6 January, IEEE, p. 156b (doi: 10.1109/HICSS.2007.206).

Parise, S 2007, 'Knowledge management and human resource development: an application in social network analysis methods', *Advances in Developing Human Resources*, vol. 9, no. 3, pp. 359–383 (doi: 10.1177/1523422307304106).

Park, P 1999, 'People, knowledge, and change in participatory research', *Management Learning*, vol. 30, no. 2, pp. 141–157.

Parsons, KM, Young, E, Butavicius, MA, McCormac, A, Pattinson, MR & Jerram, C 2015, 'The influence of organizational information security culture on information security decision making', *Journal of Cognitive Engineering and Decision Making*, vol. 9, no. 2, pp. 117–129 (doi: 10.1177/1555343415575152).

Parsons, K, McCormac, A, Butavicius, M & Ferguson, L 2010, *Human factors and information security: individual, culture and security environment*, DSTO-TR-2484, Command, Control, Communications and Intelligence Division, Defence Science and Technology Organisation, Australia, viewed 5 June 2017 <http://dspace.dsto.defence.gov.au/dspace/handle/1947/10094>.

Pascale, RT & Sternin, J 2005, 'Your company's secret change agents', *Harvard Business Review*, vol. 83, no. 5, pp. 1–12.

Paternoster, R & Simpson, S 1996, 'Sanction threats and appeals to morality: testing a rational choice model of corporate crime', *Law & Society Review*, vol. 30, no. 3, pp. 549–584.

Patriciu, V-V, Priescu, I & Nicolaescu, S 2006, 'Security metrics for enterprise information systems', *Journal of Applied Quantitative Methods*, vol. 1, no. 2, pp. 151–159.

Patterson, MG, West, MA, Shackleton, VJ, Dawson, JF, Lawthom, R, Maitlis, S, … Wallace, AM 2005, 'Validating the organizational climate measure: links to managerial practices, productivity and innovation', *Journal of Organizational Behavior*, vol. 26, pp. 379–408.

Podsakoff, PM, MacKenzie, SB, Lee, J-Y & Podsakoff, NP 2003, 'Common method biases in behavioral research: a critical review of the literature and recommended remedies', *The Journal of Applied Psychology*, vol. 88, no. 5, pp. 879–903 (doi: 10.1037/0021-9010.88.5.879).

Ponemon Institute 2016, *2016 cost of cyber crime study & the risk of business innovation*, viewed 14 November 2017, <https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf>.

Posey, C, Bennett, RJ & Roberts, TL 2011, 'Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes', *Computers & Security*, vol. 30, no. 6–7, pp. 486–497 (doi: 10.1016/j.cose.2011.05.002).

Posey, C, Bennett, RJ, Roberts, TL & Lowry, PB 2011, 'When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse', *Journal of Information System Security*, vol. 7, no. 1, pp. 24–47.

Posey, C, Roberts, TL, Lowry, PB, Courtney, J & Bennett, RJ 2011, 'Motivating the insider to protect organizational information assets: evidence from protection motivation theory and rival explanations', in *Proceedings of the Dewald Roode Workshop in Information Systems Security 2011*, pp. 1–51, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2273594>.

Posey, C, Roberts, TL, Lowry, PB & Hightower, RT 2014, 'Bridging the divide: a qualitative comparison of information security thought patterns between information security

professionals and ordinary organizational insiders', *Information and Management*, vol. 51, no. 5, pp. 551–567 (doi: http://dx.doi.org/10.1016/j.im.2014.03.009).

Puhakainen, P & Siponen, M 2010, 'Improving employees' compliance through information systems security training: an action research study', *MIS Quarterly*, vol. 34, no. 4, pp. 757–778.

Putzke, J, Fischbach, K, Schoder, D & Gloor, P 2013, 'The coevolution of network structure and perceived ease of use', in *Wirtschaftsinformatik Proceedings*, March, pp. 1541–1555.

PwC 2016, *Moving forward with cybersecurity: how organizations are adopting innovative safeguards to manage threats and achieve competitive advantage in a digital era. Key findings from the global state of information security® survey 2017*, viewed 5 June 2017, <http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf>.

Rambaran, AJ, Dijkstra, JK & Stark, TH 2013, 'Status-based influence processes: the role of norm salience in contagion of adolescent risk attitudes', *Journal of Research on Adolescence*, vol. 23, no. 3, pp. 574–585 (doi: 10.1111/jora.12032).

Raven, BH 2008, 'The bases of power and the power/interaction model of interpersonal influence', *Analyses of Social Issues and Public Policy*, vol. 8, no. 1, pp. 1–22 (doi: 10.1111/j.1530-2415.2008.00159.x).

Reagans, R & Zuckerman, EW 2001, 'Networks, diversity, and productivity: the social capital of corporate R&D teams', *Organization Science*, vol. 12, no. 4, pp. 502–517 (doi: 10.1287/orsc.12.4.502.10637).

Reason, P 2006, 'Choice and quality in action research practice', *Journal of Management Inquiry*, vol. 15, no. 2, pp. 187–203 (doi: 10.1177/1056492606288074).

Rhee, H-SS, Kim, C & Ryu, YU 2009, 'Self-efficacy in information security: its influence on end users' information security practice behavior', *Computers & Security*, vol. 28, no. 8, pp. 816–826 (doi: 10.1016/j.cose.2009.05.008).

Richardson, V 2003, 'Constructivist pedagogy', *Teachers College Record*, vol. 105, no. 9, pp. 1623–1640 (doi: 10.1046/j.1467-9620.2003.00303.x).

Riege, AM 2003, 'Validity and reliability tests in case study research: a literature review with "hands-on" applications for each research phase', *Qualitative Market Research: An International Journal*, vol. 6, no. 2, pp. 75–86.

Ripley, RM, Snijders, TAB, Boda, Z, Vörös, A & Preciado, P 2017, *Manual for RSiena*, Department of Statistics, University of Oxford and Department of Sociology, University of Groningen, viewed 14 November 2011, <http://www.stats.ox.ac.uk/~snijders/siena/RSiena_Manual.pdf>.

Roethlisberger, FJ & Dickson, WJ 1939, *Management and the worker*, Harvard University, Cambridge, MA.

Rogers, EM 1995, *Diffusion of innovations*, 3rd edn, The Free Press, New York, NY.

Rogers, RW 1975, 'A protection motivation theory of fear appeals and attitude change', *Journal of Psychology*, vol. 91, pp. 93–114.

Rowley, TJ 1997, 'Moving beyond dyadic ties: a network theory of stakeholder influences', *The Academy of Management Review*, vol. 22, no. 4, pp. 887–910 (doi: 10.5465/AMR.1997.9711022107).

Rubin, HJ & Rubin, IS 2011, *Qualitative interviewing: the art of hearing data*, SAGE Publications.

Ruighaver, AB, Maynard, SB & Chang, S 2007, 'Organisational security culture: extending the end-user perspective', *Computers & Security*, vol. 26, no. 1, pp. 56–62.

Safa, NS, von Solms, R & Futcher, L 2016, 'Human aspects of information security in organisations', *Computer Fraud & Security*, vol. 2016, no. 2, pp. 15–18 (doi: http://dx.doi.org/10.1016/S1361-3723(16)30017-3).

Safa, NS & von Solms, R 2016, 'An information security knowledge sharing model in organizations', *Computers in Human Behavior*, vol. 57, pp. 442–451 (doi: 10.1016/j.chb.2015.12.037).

Safa, NS, Sookhak, M, von Solms, R, Furnell, S, Ghani, NA & Herawan, T 2015, 'Information security conscious care behaviour formation in organizations', *Computers and Security*, vol. 53, pp. 65–78 (doi: 10.1016/j.cose.2015.05.012).

Saint-Charles, J & Mongeau, P 2009, 'Different relationships for coping with ambiguity and uncertainty in organizations', *Social Networks*, vol. 31, no. 1, pp. 33–39 (doi: 10.1016/j.socnet.2008.09.001).

Saint-Germain, R 2005, 'Information security management best practice based on ISO/IEC 17799', *Information Management Journal*, vol. 39, no. 4, pp. 60–66 (doi: 10.1055/s-0031-1297364).

Sandberg, J & Alvesson, M 2010, 'Ways of constructing research questions: gap-spotting or problematization?', *Organization*, vol. 18, no. 1, pp. 23–44 (doi: 10.1177/1350508410372151).

Sandstrom, KL, Martin, DD & Fine, GA 2014, *Symbols, selves, and social reality: a symbolic interactionist approach to social psychology and sociology*, Oxford University Press.

Sasse, MA, Brostoff, S & Weirich, D 2001, 'Transforming the "weakest link"—a human/computer interaction approach to usable and effective security', *BT Technology Journal*, vol. 19, no. 3, pp. 122–131.

Schein, EH 2010, *Organizational Culture and Leadership* (4th ed.). San Francisco (CA): Jossey-Bass.

Schlienger, T & Teufel, S 2003, 'Information security culture—from analysis to change', *South African Computer Journal*, vol. 31, pp. 46–52.

Schneider, B 1987, 'The people make the place', *Personnel Psychology*, vol. 40, no. 3, pp. 437–453.

Schneider, B, Ehrhart, MG & Macey, WH 2011, 'Organizational climate research', in NM Ashkanasy, CPM Wildrom and MF Peterson (eds), *The handbook of organizational culture and climate*, SAGE Publications, pp. 29–49.

Schneider, B, Ehrhart, MG & Macey, WH 2013, 'Organizational climate and culture', *Annual Review of Psychology*, vol. 64, pp. 361–88.

Schneider, B & Reichers, A 1983, 'On the etiology of climates', *Personnel Psychology*, vol. 1934, pp. 19–40.

Schulte, M, Cohen, N & Klein, K 2012, 'The coevolution of network ties and perceptions of team psychological safety', *Organization Science*, vol. 23, no. 2, pp. 564–581 (doi: 10.1287/orsc.1100.0582).

Schultz, E 2002, 'A framework for understanding and predicting insider attacks', *Computers & Security*, vol. 21, no. 6, pp. 526–531 (doi: https://doi.org/10.1016/S0167-4048(02)01009-X).

Scott, J 2011, 'Social network analysis: developments, advances, and prospects', *Social Network Analysis and Mining*, vol. 1, no. 1, pp. 21–26 (doi: 10.1007/s13278-010-0012-6).

Scott, J 2012, *Social network analysis: concepts, methodology, and directions for the 1990s*, SAGE Publications.

Shannon, P, Markiel, A, Ozier, O, Baliga, NS, Wang, JT, Ramage, D, Amin, N, Schwikowski, B & Ideker, T 2003, 'Cytoscape: a software environment for integrated models of biomolecular interaction networks', *Genome Research*, vol. 13, pp. 2498–2504 (doi: 10.1101/gr.1239303).

Shaw, RSS, Chen, CC, Harris, AL & Huang, H-J 2009, 'The impact of information richness on information security awareness training effectiveness', *Computers & Education*, vol. 52, no. 1, pp. 92–100 (doi: 10.1016/j.compedu.2008.06.011).

Shepard, LA 2000, 'The role of assessment in a learning culture', *Educational Researcher*, vol. 29, no. 7, pp. 4–14 (doi: 10.2307/1176145).

Shropshire, J, Warkentin, M & Sharma, S 2015, 'Personality, attitudes, and intentions: predicting initial adoption of information security behavior', *Computers & Security*, vol. 49, pp. 177–191 (doi: http://dx.doi.org/10.1016/j.cose.2015.01.002).

Silic, M & Back, A 2014a, 'Information security: critical review and future directions for research', *Information Management & Computer Security*, vol. 22, no. 3, pp. 279–308 (doi: 10.1108/IMCS-05-2013-0041).

Silic, M & Back, A 2014b, 'Shadow IT—a view from behind the curtain', *Computers & Security*, vol. 45, pp. 274–283 (doi: 10.1016/j.cose.2014.06.007).

Simmel, G 2011, *Georg Simmel on individuality and social forms*, University of Chicago Press.

Singh, N 2012, 'B.Y.O.D. genie is out of the bottle—"devil or angel" ', *Journal of Business Management & Social Sciences Research*, vol. 1, no. 3, pp. 1–12.

Siponen, M, Mahmood, MA & Pahnila, S 2014, 'Employees' adherence to information security policies: an exploratory field study', *Information & Management*, vol. 51, no. 2, pp. 217–224 (doi: http://dx.doi.org/10.1016/j.im.2013.08.006).

Siponen, M, Pahnila, S & Mahmood, A 2007, 'Employees' adherence to information security policies: an empirical study', in H Venter, M Eloff, L Labuschagne, J Eloff, and R von Solms (eds), *IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments*, Springer, Boston, MA, pp. 133–144.

Siponen, MT 2000a, 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security*, vol. 8, no. 1, pp. 31–41 (doi: 10.1108/09685220010371394).

Siponen, MT 2000b, 'Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice', *Information Management & Computer Security*, vol. 8, no. 5, pp. 197–209.

Siponen, MT 2001, 'Five dimensions of information security awareness', *Computers and Society*, vol. 31, no. 2, pp. 24–29 (doi: 10.1145/503345.503348).

Siponen, MT & Oinas-Kukkonen, H 2007, 'A review of information security issues and respective contributions', *The data base for advances in information systems*, vol. 38, no. 1, pp. 60–80 (doi: 10.1145/1216218.1216224).

Siponen, M & Vance, A 2010, 'Neutralization: new insights into the problem of employee information systems security policy violations', *MIS Quarterly*, vol. 34, no. 3, pp. 487–502.

Sopow, E 2006, ‘The impact of culture and climate on change programs’, *Strategic Communication Management*, vol. 10, no. 6, pp. 14–17.

von Solms, B 2000, ‘Information Security—The Third Wave?’, *Computers & Security*, vol. 19, vol. 7, pp. 615–620 (doi: https://doi.org/10.1016/S0167-4048(00)07021-8).

von Solms, B 2006, ‘Information security—the fourth wave’, *Computers & Security*, vol. 25, no. 3, pp. 165–168 (doi: http://dx.doi.org/10.1016/j.cose.2006.03.004).

von Solms, B 2001, ‘Information security—a multidimensional discipline’, *Computers & Security*, vol. 20, no. 6, pp. 504–508.

von Solms, B & von Solms, R 2004, ‘The 10 deadly sins of information security management’, *Computers & Security*, vol. 23, no. 5, pp. 371–376 (doi: 10.1016/j.cose.2004.05.002).

von Solms, B & Von Solms, R 2005, ‘From information security to…business security?’, *Computers & Security*, vol. 24, no. 4, pp. 271–273 (doi: http://dx.doi.org/10.1016/j.cose.2005.04.004).

von Solms, R & van Niekerk, J 2013, ‘From information security to cyber security’, *Computers and Security*, vol. 38, pp. 97–102 (doi: 10.1016/j.cose.2013.04.004).

Sommestad, T, Hallberg, J, Lundholm, K & Bengtsson, J 2014, ‘Variables influencing information security policy compliance: a systematic review of quantitative studies’, *Information Management & Computer Security*, vol. 22, no. 1, pp. 42–75 (doi: 10.1108/IMCS-08-2012-0045).

Sommestad, T, Karlzén, H & Hallberg, J 2015a, ‘A meta-analysis of studies on protection motivation theory and information security behaviour’, *International Journal of Information Security and Privacy*, vol. 9, no. 1, pp. 26–46 (doi: 10.4018/IJISP.2015010102).

Sommestad, T, Karlzén, H & Hallberg, J 2015b, ‘The sufficiency of the theory of planned behavior for explaining information security policy compliance’, *Information & Computer Security*, vol. 23, no. 2, pp. 200–217 (doi: http://dx.doi.org/10.1108/ICS-01-2015-0001).

Son, J-Y 2011, 'Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies', *Information & Management*, vol. 48, no. 7, pp. 296–302.

Sparrowe, RT, Liden, RC, Wayne, SJ & Kraimer, ML 2001, 'Social networks and the performance of individuals and groups', *The Academy of Management Journal*, vol. 44, no. 2, pp. 316–325.

Spears, J 2006, 'A holistic risk analysis method for identifying information security risks', in P Downland, S Furnell, B Thuraisingham and XS Wang (eds), *Security management, integrity, and internal control in information systems*, Springer, pp. 185–202.

Spears, J & Barki, H 2010, 'User participation in information systems security risk management', *MIS Quarterly*, vol. 34, no. 3, pp. 503–522.

Spurling, P 1995, 'Promoting security awareness and commitment', *Information Management & Computer Security*, vol. 3, no. 2, pp. 20–26 (doi: 10.1108/09685229510792988).

Stanton, JM, Stam, KR., Guzman, I & Caledra, C 2003, 'Examining the linkage between organizational commitment and information security', in *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics*, vol. 3 (Cat. No.03CH37483), IEEE, pp. 2501–2506 (doi: 10.1109/ICSMC.2003.1244259).

Stanton, JM, Stam, KR, Mastrangelo, P & Jolton, J 2005, 'Analysis of end user security behaviors', *Computers & Security*, vol. 24, no. 2, pp. 124–133.

Steglich, C, Snijders, TAB & Pearson, M 2010, 'Dynamic networks and behaviour: separating selection from influence', *Sociological Methodology*, vol. 40, no. 1, pp. 329–393 (doi: 10.1111/j.1467-9531.2010.01225.x).

Straub, DW 1990, 'Effective IS security: an empirical study', *Information Systems Research*, vol. 1, no. 3, pp. 255–276.

Straub, DW & Welke, RJ 1998, 'Coping with systems risk: security planning models for management decision making', *MIS Quarterly*, vol. 22, no. 4, pp. 441–469 (doi: 10.2307/249551).

Susman, GI & Evered, RD 1978, ‘An assessment of the scientific merits of action research’, *Administrative Science Quarterly*, vol. 23, no. 4, p. 582–603 (doi: 10.2307/2392581).

Sykes, T, Venkatesh, V & Gosain, S 2009, ‘Model of acceptance with peer support: a social network perspective to understand employees’ system use’, *MIS Quarterly*, vol. 33, no. 2, pp. 371–393.

Symantec 2017, *Internet security threat report*, viewed 5 June 2017, <https://www.symantec.com/security-center/threat-report>.

TCKT 2011, ‘TTT Architects và Giải thưởng dành cho tinh thần đồng đội’, *Tap Chi Kien Truc*, 20 March 2011, viewed 14 November 2017, <https://www.tapchikientruc.com.vn/cuoc-thi/ct-trong-nuoc/ttt-architects-va-giai-thuong-danh-cho-tinh-than-dong-doi.html>.

Thomas, E & Magilvy, JK 2011, ‘Qualitative rigor or research validity in qualitative research’, *Journal for Specialists in Pediatric Nursing*, vol. 16, no. 2, pp. 151–155 (doi: 10.1111/j.1744-6155.2011.00283.x).

Thomson, G 2012,. ‘BYOD: enabling the chaos’, *Network Security*, vol. 2012, no. 2, pp. 5–8.

Thomson, K, von Solms, R & Louw, L 2006, ‘Cultivating an organizational information security culture’, *Computer Fraud & Security*, vol. 2006, no. 10, pp. 7–11 (doi: https://doi.org/10.1016/S1361-3723(06)70430-4).

Thomson, K, von Solms, R & Technikon, PE 2006, ‘Towards an information security competence maturity model’, *Computer Fraud & Security*, vol. 5, pp. 11–15 (doi: http://dx.doi.org/10.1016/S1361-3723(06)70356-6).

Thomson, ME & von Solms, R 1998, ‘Information security awareness: educating your users effectively’, *Information Management & Computer Security*, vol. 6, no. 4, pp. 167–173 (doi: 10.1108/09685229810227649).

Tichy, NM, Tushman, ML & Fombrun, C 1979, ‘Social network analysis for organizations’, *The Academy of Management Review*, vol. 4, no. 4, pp. 507–519 (doi: 10.2307/257851).

de Toni, AF & Nonino, F 2010, 'The key roles in the informal organization: a network analysis perspective', *The Learning Organization*, vol. 17, no. 1, pp. 86–103 (doi: 10.1108/09696471011008260).

Torres, JM, Sarriegi, JM, Santos, J & Serrano, N 2006, 'Managing information systems security : critical success factors and indicators to measure effectiveness', in SK Katsikas, J López, M Backes, S Gritzalis, B Preneel (eds) *Information Security. ISC 2006. Lecture Notes in Computer Science, vol 4176*. Springer Berlin Heidelbergpp, pp. 530–545.

Tsohou, A, Karyda, M, Kokalakis, S & Kiontouzis, E 2013, 'Managing the introduction of information security awareness programmes in organisations', *European Journal of Information Systems*, vol. 24, no. 1, Nature Publishing Group, pp. 1–21 (doi: 10.1057/ejis.2013.27).

TTT Corporation 2017, *TTT Corporation - Awards*, viewed 23 June 2017, <http://ttt.vn/AboutTTT/Awards.aspx>.

Tuoi Tre News 2017, 'Almost 7,700 cyber attacks on Vietnamese websites since January: report', 23 March 2017, viewed 5 June 2017, <http://tuoitrenews.vn/society/40167/7700-cyber-attacks-on-vietnamese-websites-since-january-report>.

Umphress, EE, Labianca, G, Brass, DJ, Kass, E & Scholten, L 2003, 'The role of instrumental and expressive social ties in employees' perceptions of organizational justice', *Organization Science*, vol. 14, no. 6, pp. 738–753.

Urquhart, C & Lennox, M 1999, 'Perceptions and adoption of IT: conversations in agriculture', in *Proceedings of 10th Australasian Conference on Information Systems*, pp. 1059–1070.

Valente, TW 1996, 'Social network thresholds in the diffusion of innovations', *Social Networks*, vol. 18, no. 1, pp. 69–89 (doi: 10.1016/0378-8733(95)00256-1).

Valente, TW 2012, 'Network interventions', *Science*, vol. 337, no. 6090, pp. 49–53 (doi: 10.1126/science.1217330).

Valente, TW & Davis, RL 1999, 'Accelerating the diffusion of innovations using opinion leaders', *The Annals of the American Academy of Political and Social Science*, vol. 566, pp. 55–67.

Valente, TW, Palinkas, LA, Czaja, S, Chu, K-H & Brown, CH 2015, 'Social network analysis for program implementation', *PLoS ONE*, vol. 10, no. 6, p. e0131712 (doi: 10.1371/journal.pone.0131712).

Valente, TW & Pumpuang, P 2007, 'Identifying opinion leaders to promote behavior change', *Health Education & Behavior*, vol. 34, no. 6, pp. 881–896 (doi: 10.1177/1090198106297855).

Vance, A, Siponen, M & Pahnila, S 2012, 'Motivating IS security compliance: insights from habit and protection motivation theory', *Information & Management*, vol. 49, no. 3–4, pp. 190–198 (doi: http://dx.doi.org/10.1016/j.im.2012.04.002).

da Veiga, A & Eloff, JHP 2007, 'An information security governance framework', *Information Systems Management*, vol. 24, no. 4, pp. 361–372 (doi: 10.1080/10580530701586136).

da Veiga, A & Eloff, JHP 2010, 'A framework and assessment instrument for information security culture', *Computers & Security*, vol. 29, no. 2, pp. 196–207 (doi: http://dx.doi.org/10.1016/j.cose.2009.09.002).

da Veiga, A & Martins, N 2015, 'Improving the information security culture through monitoring and implementation actions illustrated through a case study', *Computers & Security*, vol. 49, pp. 162–176 (doi: http://dx.doi.org/10.1016/j.cose.2014.12.006).

Venkatesh, V, Morris, MG, Davis, GB & Davis, FD 2003, 'User acceptance of information technology: toward a unified view', *MIS Quarterly*, vol. 27, no. 2, pp. 452–478.

Vidgen, R, Madsen, S & Kautz, K 2004, 'Mapping the information system development process', in B Fitzgerald B and E Wynn (eds), *IT Innovation for Adaptability and Competitiveness, TDIT 2004, IFIP International Federation for Information Processing, vol 141*, Springer, Boston, MA, pp. 157–171.

Vietnam MIC 2014, *Vietnam information and data on information and communication technology. Whitebook 2014*, Ministry of Information and Communication, Hanoi,

Vietnam, viewed 15 September 2016, <http://english.mic.gov.vn/Upload/Store/tintuc/vietnam/43/Sach-Trang-2014-final.pdf>.

VietNamNet Bridge 2017, 'Vietnam needs to promote ICT to grab opportunities for development: Minister', 20 March 2017, viewed 15 September 2016, <http://english.vietnamnet.vn/fms/science-it/174875/vietnam-needs-to-promote-ict-to-grab-opportunities-for-development---minister.html>.

Vinh, LQ 2015, ' "Nhà Quốc hội" đoạt giải Lớn Giải thưởng Kiến trúc quốc gia 2014', *Lao Dong*, 18 April 2015, viewed 14 November 2016, <http://laodong.com.vn/van-hoa/nha-quoc-hoi-doat-giai-lon-giai-thuong-kien-truc-quoc-gia-2014-317503.bld>.

Wallace, MJ 1998, 'Why action research?', *Action Research*, vol. 1, no. 1, pp. 9–28.

Walters, R 2013, 'Bringing IT out of the shadows', *Network Security*, vol. 2013, no. 4, pp. 5–11 (doi: 10.1016/S1353-4858(13)70049-7).

Warkentin, M, Johnston, AC & Shropshire, J 2011, 'The influence of the informal social learning environment on information privacy policy compliance efficacy and intention', *European Journal of Information Systems*, vol. 20, no. 3, pp. 267–284 (doi: 10.1057/ejis.2010.72).

Warkentin, M, Johnston, AC, Shropshire, J & Barnett, WD 2016, 'Continuance of protective security behavior: a longitudinal study', *Decision Support Systems*, vol. 92, pp. 25–35 (doi: http://dx.doi.org/10.1016/j.dss.2016.09.013).

Warkentin, M & Mutchler, L 2014, 'Behavioral information security management', in G Tucker and D-H Topi (eds), *Computing handbook*, 3rd edn, Taylor & Francis Group, pp. 1–14.

Warkentin, M & Willison, R 2009, 'Behavioral and policy issues in information systems security: the insider threat', *European Journal of Information Systems*, vol. 18, no. 2, pp. 101–105.

Warner, WL & Lunt, PS 1941, *The social life of a modern community*, Yale University Press, New Haven, CT.

Wasserman, S & Faust, K 1994, *Social network analysis: methods and applications*, Cambridge University Press.

Weick, KE 1995, *Sensemaking in organizations*, SAGE Publications, Thousand Oaks, CA.

Wellman, B 1983, 'Network analysis: some basic principles', *Sociological Theory*, vol. 1, no. 1983, pp. 155–200 (doi: 10.2307/202050).

White, M 2012, 'Digital workplaces: vision and reality', *Business Information Review*, vol. 29, no. 4, pp. 205–214.

Willison, R & Warkentin, M 2013, 'Beyond deterrence: an expanded view of employee computer abuse', *MIS Quarterly*, vol. 37, no. 1, pp. 1–20.

Wilson, JLL, Turban, E & Zviran, M 1992, 'Information systems security: a managerial perspective', *International Journal of Information Management*, vol. 12, no. 2, pp. 105–119 (doi: 10.1016/0268-4012(92)90017-K).

Wilson, M & Hash, J 2003, *Building an information technology security awareness and training program*, NIST Special Publication 800-50, U.S. Department of Commerce, viewed 5 June 2017, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf>.

Wölfer, R & Scheithauer, H 2014, 'Social influence and bullying behavior: intervention-based network dynamics of the fairplayer.manual bullying prevention program', *Aggressive Behavior*, vol. 40, no. 4, pp. 309–319 (doi: 10.1002/ab.21524).

Wood, CC 2000, 'An unappreciated reason why information security policies fail', *Computer Fraud & Security*, vol. 2000, no. 10, pp. 13–14 (doi: http://dx.doi.org/10.1016/S1361-3723(00)10029-6).

Wood, CC & Banks Jr, WW 1993, 'Human error: an overlooked but significant information security problem', *Computers & Security*, vol. 12, no. 1, pp. 51–60 (doi: http://dx.doi.org/10.1016/0167-4048(93)90012-T).

Workman, M, Bommer, WH & Straub, D 2008, 'Security lapses and the omission of information security measures: a threat control model and empirical test', *Computers*

in Human Behavior, vol. 24, no. 6, pp. 2799–2816 (doi: http://dx.doi.org/10.1016/j.chb.2008.04.005).

Wu, Y & Saunders, CS 2011, 'Governing information security: governance domains and decision rights allocation patterns', *Information Resources Management Journal*, vol. 24, no. 1, pp. 28–45 (doi: 10.4018/irmj.2011010103).

Yazdanmehr, A & Wang, J 2016, 'Employees' information security policy compliance: a norm activation perspective', *Decision Support Systems*, vol. 92, pp. 36–46 (doi: http://dx.doi.org/10.1016/j.dss.2016.09.009).

Yilmaz, K 2008, 'Constructivism: its theoretical underpinnings, variations, and implications for classroom instruction', *Educational Horizons*, vol. 86, no. 3, pp. 161–172.

Yin, RK 2009, *Case study research design and methods*, 4th edn, SAGE Publications, Thousand Oaks, CA.

Yoo, CW & Sanders, GL 2013, 'An exploration of group information security compliance: a social network analysis perspective', in the *Thirty-Fourth International Conference on Information Systems 2013*, <http://aisel.aisnet.org/icis2013/proceedings/ResearchInProgress/18/>.

Zafar, H 2013, 'Human resource information systems: information security concerns for organizations', *Human Resource Management Review*, vol. 23, no. 1, pp. 105–113 (doi: http://dx.doi.org/10.1016/j.hrmr.2012.06.010).

Zafar, H & Clark, JG 2009, 'Current state of information security research in IS', *Communications of the Association for Information Systems*, vol. 24, no. 1, pp. 557–596.

Zhang, J, Reithel, BJ & Li, H 2009, 'Impact of perceived technical protection on security behaviors', *Information Management & Computer Security*, vol. 17, no. 4, pp. 330–340 (doi: 10.1108/09685220910993980).

Zheng, K, Padman, R, Krackhardt, D, Johnson, MP & Diamond, HS 2010, 'Social networks and physician adoption of electronic health records: insights from an empirical study', *Journal of the American Medical Informatics Association*, vol. 17, no. 3, pp. 328–36.

Zhou, S, Siu, F & Wang, M 2010, 'Effects of social tie content on knowledge transfer', *Journal of Knowledge Management*, vol. 14, no. 3, pp. 449–463 (doi: 10.1108/13673271011050157).

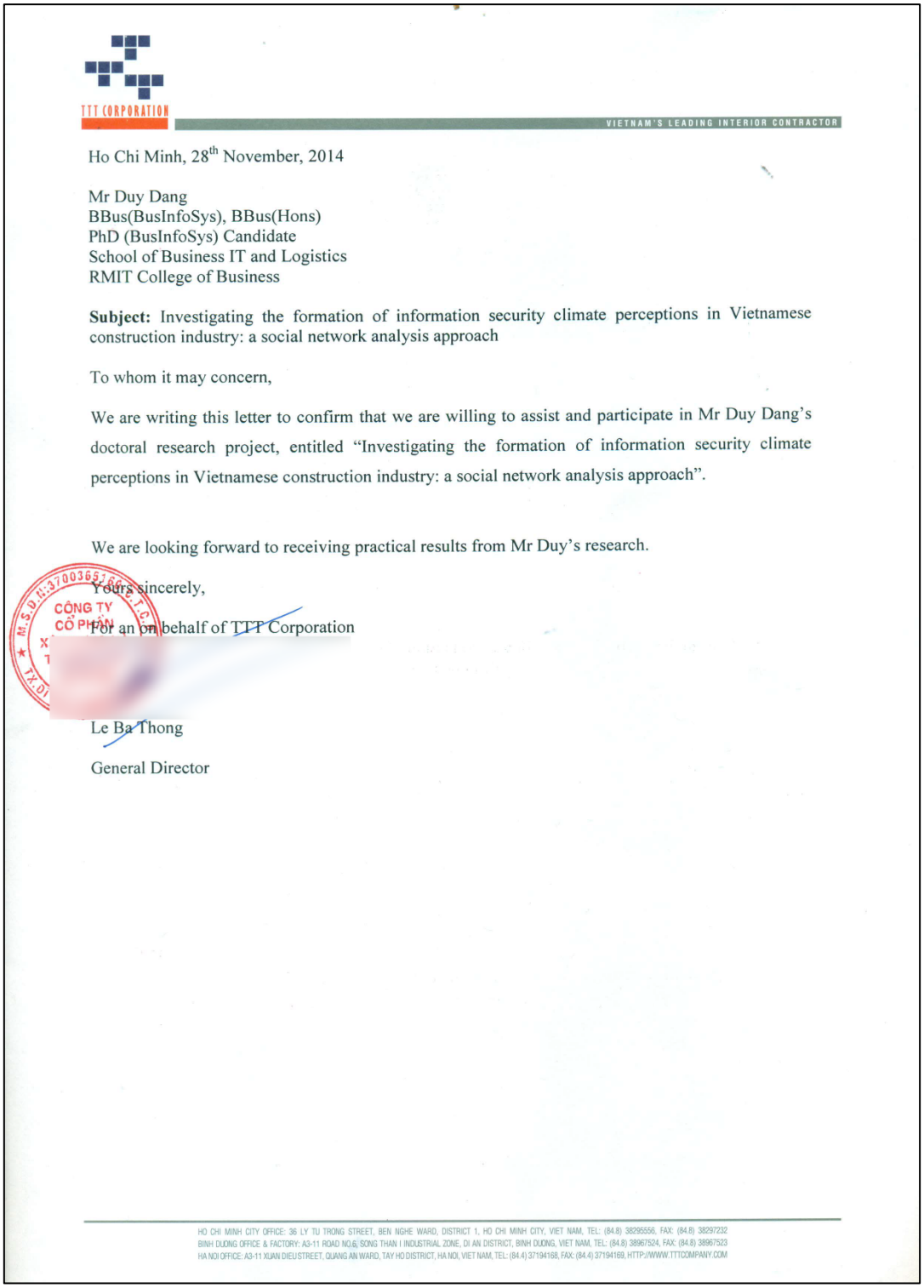
Zohar, D 2010, 'Thirty years of safety climate research: reflections and future directions', *Accident Analysis and Prevention*, vol. 42, no. 5, pp. 1517–1522.

Zohar, D 2014, 'Safety climate: conceptualization, measurement, and improvement', in B Schneider and KM Barbera (eds), *The Oxford Handbook of Organizational Climate and Culture*, Oxford University Press, UK, pp. 317–334.

Zohar, D & Luria, G 2005, 'A multilevel model of safety climate: cross-level relationships between organization and group-level climates', *The Journal of Applied Psychology*, vol. 90, no. 4, pp. 616–628 (doi: 10.1037/0021-9010.90.4.616).

Appendices

Appendix A. Research Agreements



TTT CORPORATION

VIETNAM'S LEADING INTERIOR CONTRACTOR

Ho Chi Minh, 28th November, 2014

Mr Duy Dang
BBus(BusInfoSys), BBus(Hons)
PhD (BusInfoSys) Candidate
School of Business IT and Logistics
RMIT College of Business

Subject: Investigating the formation of information security climate perceptions in Vietnamese construction industry: a social network analysis approach

To whom it may concern,

We are writing this letter to confirm that we are willing to assist and participate in Mr Duy Dang's doctoral research project, entitled "Investigating the formation of information security climate perceptions in Vietnamese construction industry: a social network analysis approach".

We are looking forward to receiving practical results from Mr Duy's research.

Yours sincerely,
For an on behalf of TTT Corporation

Le Ba Thong

General Director

HO CHI MINH CITY OFFICE: 36 LY TU TRONG STREET, BEN NGHE WARD, DISTRICT 1, HO CHI MINH CITY, VIET NAM, TEL: (84.8) 38295556, FAX: (84.8) 38297232
BINH DUONG OFFICE & FACTORY: A3-11 ROAD NO.6, SONG THAN I INDUSTRIAL ZONE, DI AN DISTRICT, BINH DUONG, VIET NAM, TEL: (84.8) 38967524, FAX: (84.8) 38967523
HA NOI OFFICE: A3-11 XUAN DIEU STREET, QUANG AN WARD, TAY HO DISTRICT, HA NOI, VIET NAM, TEL: (84.4) 37194168, FAX: (84.4) 37194169, HTTP://WWW.TTTCOMPANY.COM

Figure A.1. Letter of Approval to Conduct Research with TTT Corporation

THỎA THUẬN NGHIÊN CỨU
RESEARCH AGREEMENT

V/v: Thực hiện đề tài Nghiên cứu dự án Tiến sĩ tại Công ty TTT
RE: Conducting PhD research project at TTT Corporation

Căn cứ thỏa thuận giữa **Ông Đặng Phạm Thiên Duy** và **Công ty Cổ phần Xây dựng và Thương mại TTT** về việc hợp tác nghiên cứu phát triển công nghệ bảo mật thông tin và căn cứ khả năng của ông Đặng Phạm Thiên Duy;
*According to the agreement between **Mr Dang Pham Thien Duy** and **TTT Corporation** about the research collaboration to improve TTT Corporation's information security management system and to the best of Mr Duy's ability;*

Hôm nay, ngày 28 tháng 11 năm 2014, tại Công ty TTT, chúng tôi gồm có:
Today, 28th of November, 2014 at TTT Corporation, we are:

BÊN A: **Ông Đặng Phạm Thiên Duy** – Gọi tắt là Bên A
*PARTY A: **Mr Dang Pham Thien Duy** – hereby known as Party A*

Chức vụ: Sinh viên nghiên cứu (chính) của dự án Tiến sĩ tại Đại Học RMIT
Position: Principal student investigator of PhD research project at RMIT University

Địa chỉ: 702/9 Earl Street, Carlton VIC 3053, Melbourne, Australia
Address: 702/9 Earl Street, Carlton VIC 3053, Melbourne, Australia

Điện thoại: +61 490 027 759
Phone number: +61 490 027 759

BÊN B: **Công ty Cổ phần Xây dựng và Thương mại TTT** – Gọi tắt là Bên B
*PARTY B: **TTT Corporation** – hereby known as Party B*

Đại diện: Ông Lê Bá Thông – Chức vụ: Tổng Giám Đốc
Represented by: Mr Le Ba Thong – Position: General Director

Địa chỉ: 36 Lý Tự Trọng, P. Bến Nghé, Q1
Address: 36 Ly Tu Trong, Ben Nghe Ward, District 1, Ho Chi Minh City, Vietnam

Điện thoại: +84 8 3829 5556
Phone number: +84 8 3829 5556

Figure A.2. Research Agreement with TTT Corporation (Page 1 of 4)

Hai bên A, B thực hiện ký Thỏa Thuận Nghiên Cứu với những điều khoản sau:
The parties A and B both sign this RESEARCH AGREEMENT for the following sections and terms:

ĐIỀU 1: ĐIỀU KHOẢN CHUNG:
SECTION 1: GENERAL TERMS:

- Bên A đồng ý với Bên B để ký kết Thỏa Thuận Nghiên Cứu và hoàn thành dự án Tiến sĩ với đề tài **"Tìm hiểu quá trình hình thành môi trường bảo mật trong công ty xây dựng Việt Nam: Áp dụng phương pháp phân tích mạng xã hội".**
  *Party A agrees with Party B to sign the RESEARCH AGREEMENT and complete the PhD research project entitled "**Investigating the formation of information security climate in Vietnamese construction industry: a social network analysis approach**".*

- Thời gian hiệu lực: Bắt đầu từ ngày ký biên bản này đến khi dự án nghiên cứu Tiến sĩ nêu trên được hoàn tất vào tháng 3 năm 2018.
  Effective time: from the signing date of this agreement until the mentioned PhD research project is completed by March 2018.

ĐIỀU 2: TRÁCH NHIỆM CỦA CÁC BÊN:
SECTION 2: RESPONSIBILITIES:

1. **Trách nhiệm của Ông Đặng Phạm Thiên Duy**:
   Responsibilities of Mr. Dang Pham Thien Duy

   - Cung cấp kết quả khảo sát sau khi đã xóa bỏ thông tin của người tham gia khảo sát. *Provide the research survey's findings after anonymise and/or remove the identifiable information of the survey*

   - Chỉ dùng cho mục đích nghiên cứu (vd. xuất bản trong luận án Tiến sĩ, các thông cáo hội nghị và tạp chí khoa học) và không được chuyển dữ liệu khảo sát cho các bên thứ Ba với mục đích phi học thuật hay không nhằm vào nghiên cứu.
     Use only the research survey's findings for research purposes (i.e. publishing in a doctoral thesis, conference proceedings and scientific journals) and NOT disclose the research survey's findings to any third parties for non-research purposes.

2. **Quyền lợi và trách nhiệm của Ông Lê Bá Thông:**
   Responsibilities of Mr. Le Ba Thong

   - Đôn đốc toàn thể nhân viên hoàn thành bảng khảo sát đúng thời hạn Bên A yêu cầu.
     Encourage TTT Corporation's employees to participate in the research survey within the timeframe suggested by Party A.

Figure A.3. Research Agreement with TTT Corporation (Page 2 of 4)

- Được quyền xem kết quả khảo sát sau khi đã xóa bỏ thông tin của người tham gia khảo sát.
  Can request access to the research survey's findings after the identifiable information of the participants has been anonymised and/or removed.
- Cho phép Bên A nhắc đến tên của TTT Corporation và đại diện Bên B, cũng như các hình ảnh đính kèm trong Phụ lục của thỏa thuận này, trong luận án Tiến sĩ hoàn thành bởi đại diện Bên a
  Allow Party A to mention the names of TTT Corporation and Party B's representative, as well as the photos attached in this agreement's Appendix, in the PhD research thesis prepared by Party A's representative.
- Trong trường hợp chủ đề tài không thực hiện theo thỏa thuận trong biên bản, Bên A phải chịu trách nhiệm hủy toàn bộ kết quả của cuộc khảo sát.
  In the event that Party A breaches any terms of this agreement, Party A is responsible for destroying the research survey's finding.

ĐIỀU 3: ĐIỀU KHOẢN THỰC HIỆN:

SECTION 3: COMPLIANCE WITH THE TERMS:

Biên bản được lập thành 2 bản có giá trị như nhau, mỗi bên liên quan giữ 01 bản. Hai bên có trách nhiệm thực hiện những gì đã cam kết trong biên bản này. Trong quá trình thực hiện, nếu có vấn đề chưa thống nhất hoặc cần bổ sung, thay đổi, hai bên có trách nhiệm bàn bạc để cùng nhau giải quyết.

This agreement has 2 copies that hold equal value, and each party receive and keep one copy. Both parties are responsible for complying with the terms as specified in this agreement. During the research project, if there are additional conditions or disputes, both parties are responsible for discussing and reaching a resolution.

Ông Đặng Phạm Thiên Duy	**Công ty TTT**
(BÊN A)	**(BÊN B)**
	LÊ BÁ THÔNG
	GENERAL DIRECTOR

Figure A.4. Research Agreement with TTT Corporation (Page 3 of 4)

PHỤ LỤC:

APPENDIX:

Figure 1: The project management and construction departments in the headquarters building

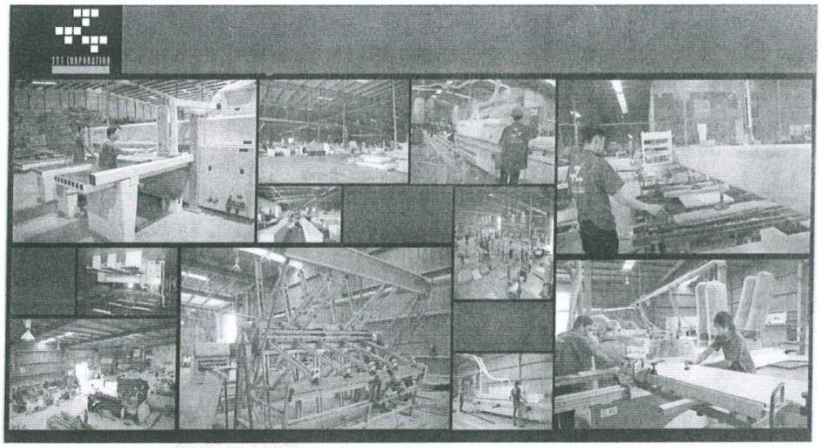
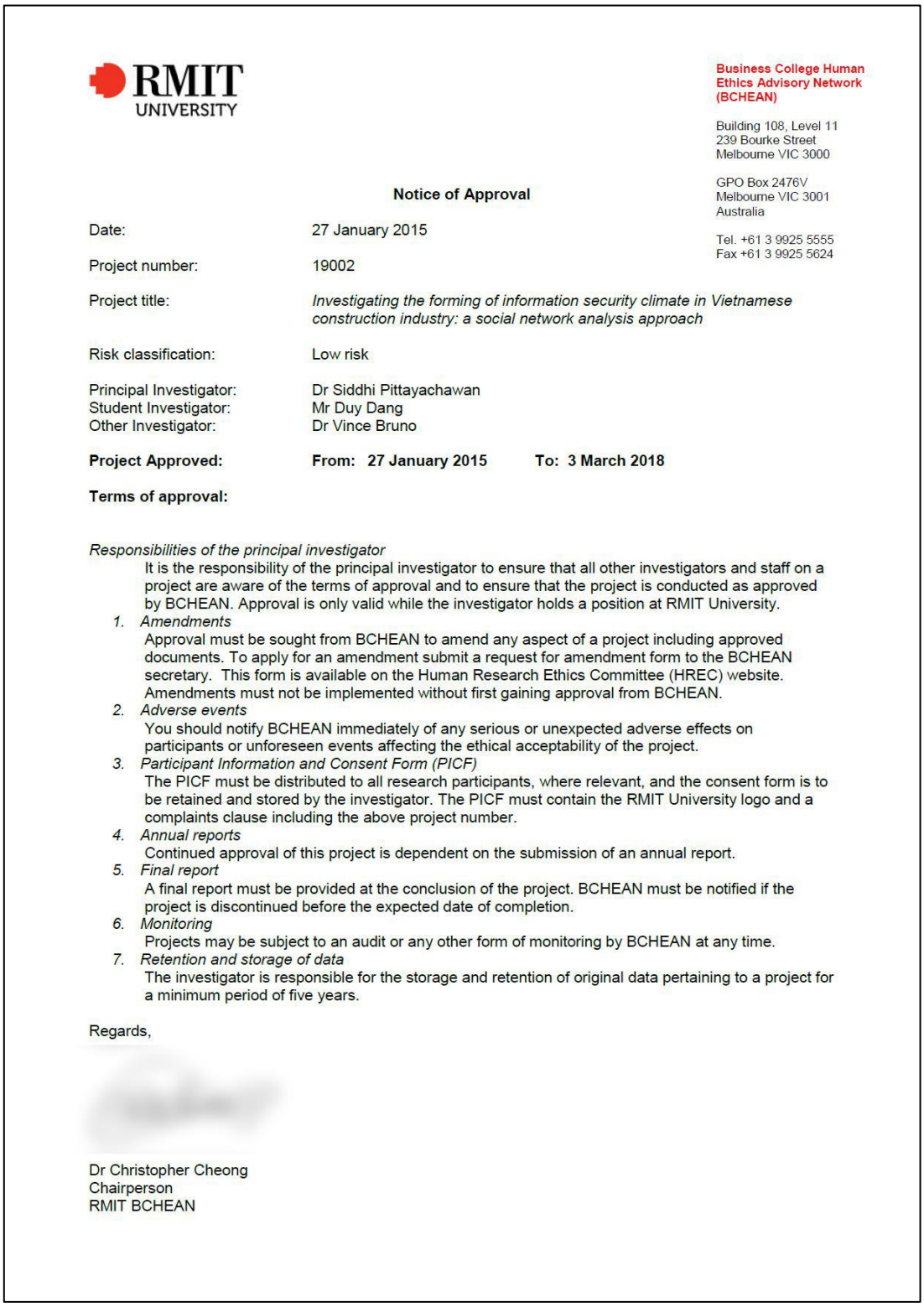


Figure 2: Factory division in Binh Duong, a suburb of Ho Chi Minh City

Figure A.5. Research Agreement with TTT Corporation (Page 4 of 4)

Appendix B. Ethics Approvals



RMIT UNIVERSITY

Business College Human Ethics Advisory Network (BCHEAN)

Building 108, Level 11
239 Bourke Street
Melbourne VIC 3000

GPO Box 2476V
Melbourne VIC 3001
Australia

Tel. +61 3 9925 5555
Fax +61 3 9925 5624

Notice of Approval

Date:	27 January 2015
Project number:	19002
Project title:	*Investigating the forming of information security climate in Vietnamese construction industry: a social network analysis approach*
Risk classification:	Low risk
Principal Investigator:	Dr Siddhi Pittayachawan
Student Investigator:	Mr Duy Dang
Other Investigator:	Dr Vince Bruno
Project Approved:	**From: 27 January 2015 To: 3 March 2018**

Terms of approval:

Responsibilities of the principal investigator

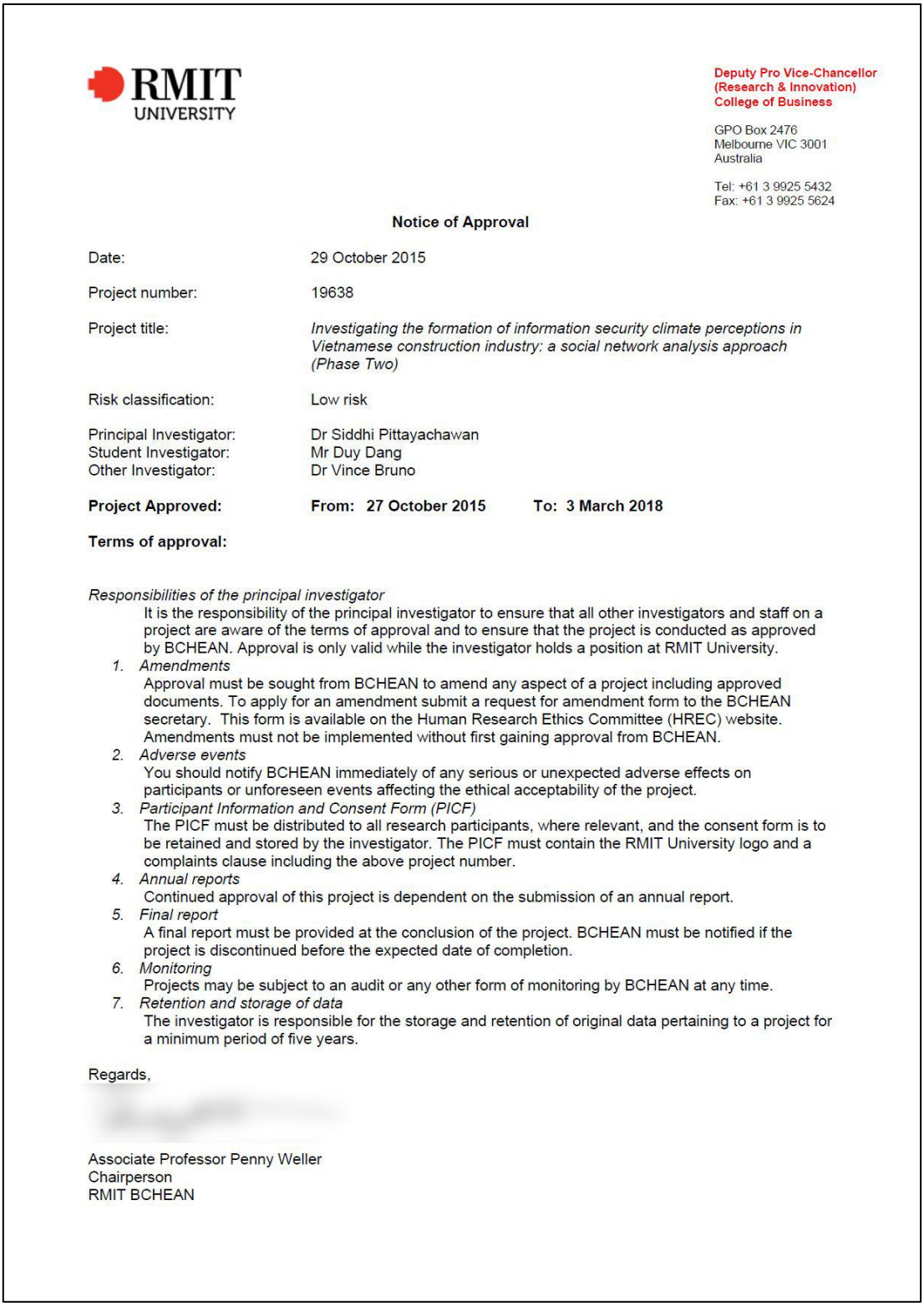
It is the responsibility of the principal investigator to ensure that all other investigators and staff on a project are aware of the terms of approval and to ensure that the project is conducted as approved by BCHEAN. Approval is only valid while the investigator holds a position at RMIT University.

1. *Amendments*
   Approval must be sought from BCHEAN to amend any aspect of a project including approved documents. To apply for an amendment submit a request for amendment form to the BCHEAN secretary. This form is available on the Human Research Ethics Committee (HREC) website. Amendments must not be implemented without first gaining approval from BCHEAN.
2. *Adverse events*
   You should notify BCHEAN immediately of any serious or unexpected adverse effects on participants or unforeseen events affecting the ethical acceptability of the project.
3. *Participant Information and Consent Form (PICF)*
   The PICF must be distributed to all research participants, where relevant, and the consent form is to be retained and stored by the investigator. The PICF must contain the RMIT University logo and a complaints clause including the above project number.
4. *Annual reports*
   Continued approval of this project is dependent on the submission of an annual report.
5. *Final report*
   A final report must be provided at the conclusion of the project. BCHEAN must be notified if the project is discontinued before the expected date of completion.
6. *Monitoring*
   Projects may be subject to an audit or any other form of monitoring by BCHEAN at any time.
7. *Retention and storage of data*
   The investigator is responsible for the storage and retention of original data pertaining to a project for a minimum period of five years.

Regards,

Dr Christopher Cheong
Chairperson
RMIT BCHEAN

Figure B.1. Ethics Approval for Data Collection (Case Study)



RMIT UNIVERSITY

Deputy Pro Vice-Chancellor
(Research & Innovation)
College of Business

GPO Box 2476
Melbourne VIC 3001
Australia

Tel: +61 3 9925 5432
Fax: +61 3 9925 5624

Notice of Approval

Date:	29 October 2015
Project number:	19638
Project title:	*Investigating the formation of information security climate perceptions in Vietnamese construction industry: a social network analysis approach (Phase Two)*
Risk classification:	Low risk
Principal Investigator: Student Investigator: Other Investigator:	Dr Siddhi Pittayachawan Mr Duy Dang Dr Vince Bruno
Project Approved:	**From: 27 October 2015 To: 3 March 2018**

Terms of approval:

Responsibilities of the principal investigator

It is the responsibility of the principal investigator to ensure that all other investigators and staff on a project are aware of the terms of approval and to ensure that the project is conducted as approved by BCHEAN. Approval is only valid while the investigator holds a position at RMIT University.

1. *Amendments*
   Approval must be sought from BCHEAN to amend any aspect of a project including approved documents. To apply for an amendment submit a request for amendment form to the BCHEAN secretary. This form is available on the Human Research Ethics Committee (HREC) website. Amendments must not be implemented without first gaining approval from BCHEAN.
2. *Adverse events*
   You should notify BCHEAN immediately of any serious or unexpected adverse effects on participants or unforeseen events affecting the ethical acceptability of the project.
3. *Participant Information and Consent Form (PICF)*
   The PICF must be distributed to all research participants, where relevant, and the consent form is to be retained and stored by the investigator. The PICF must contain the RMIT University logo and a complaints clause including the above project number.
4. *Annual reports*
   Continued approval of this project is dependent on the submission of an annual report.
5. *Final report*
   A final report must be provided at the conclusion of the project. BCHEAN must be notified if the project is discontinued before the expected date of completion.
6. *Monitoring*
   Projects may be subject to an audit or any other form of monitoring by BCHEAN at any time.
7. *Retention and storage of data*
   The investigator is responsible for the storage and retention of original data pertaining to a project for a minimum period of five years.

Regards,

Associate Professor Penny Weller
Chairperson
RMIT BCHEAN

Figure B.2. Ethics Approval for Data Collection (Network Surveys)

Appendix C. Case Study Interview Questions

The following questions were used as part of the interviews with the InfoSec experts in the diagnosis stage:

1) Please tell me about your experiences in the InfoSec industry and your role in your organisation.
2) How popular or common are InfoSec standards such as ISO, COBIT and ITIL in the Vietnamese industry?
3) Please describe the steps of how you implemented the ISO 27001 standard in your company. What are the key factors in each of these steps?
4) What are the key factors for building an effective InfoSec work environment?

As the experts answer the above questions, I asked them to elaborate on the important concepts that they mentioned. For example:

- How to motivate employees' InfoSec compliance?
- Why do employees refuse to comply with InfoSec policy?
- What are the pros and cons of different approaches and tools to motivate InfoSec compliance?
- What does the interviewee mean by 'InfoSec champions', and how to select these champions?

Appendix D. Conducting ERGM Analysis

ERGM involves specifying a mathematical model with terms that potentially explain the forming process of ties within an observed network, then evaluating the model and assessing the model's goodness-of-fit. In the action planning stage of the CAR project I analysed three models which described the InfoSec influence network and its forming mechanisms.

The questionnaire (see Table 6.1), which asked the respondents to nominate their ties with others, collected data about the observed networks. The observed network of InfoSec influence was considered as only one pattern out of many possible patterns, and my goal was to specify a model that could be used to reliably create simulated networks that would resemble the observed network. To this end, I specified a combination of sensible terms describing the forming mechanisms of the observed network. The inclusion of the terms was based on the discussed theoretical background (see Section 6.2.1) and the descriptive analysis which showed the InfoSec influence network's distinctive characteristics such as reciprocity, centralisation and transitivity (see Section 6.3.1).

Specification of models

The strategy for specifying the models was as follows. First, I included the terms that described the effects of employees' background characteristics, which were age, gender, tenure, seniority and department membership, on the occurrence of InfoSec influence ties. This model, Model 1, described the inherent personal characteristics that made an employee influence or have InfoSec behaviours influenced by others.

Second, employees' socialisation, which was defined through the provisions of instrumental, expressive and InfoSec support resources, was included in a second model, Model 2. These terms about the effects of employees' socialisation were specified together with the terms about the background characteristics' effects. Model 2 took into account the socialisation that allowed employees to project social powers onto their colleagues and influence their InfoSec behaviours, as suggested by the theory of social power bases (Raven 2008) and the mechanisms of social influence (Cialdini & Goldstein 2004; Kelman 1961; Leenders 2002).

Third, I specified a model that combined all the terms of Models 1 and 2 with those about the InfoSec influence network's structural characteristics such as transitivity and reciprocity. This model, Model 3, simultaneously evaluated all of the effects caused by employees' background

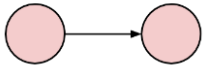
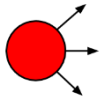
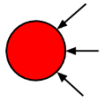
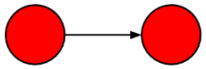
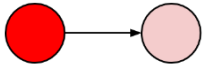
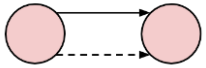
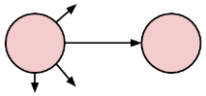
characteristics, their socialisation and the InfoSec influence network's structural characteristics on the occurrence of InfoSec influence ties.

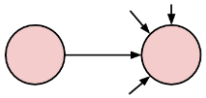
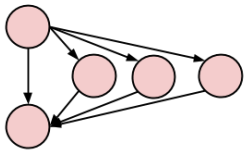
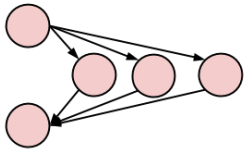
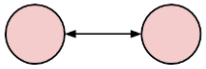
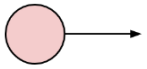
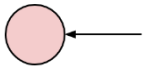
The purpose of this strategy for specifying models was to progressively evaluate the effects of employees' background characteristics on InfoSec influence (Model 1), then the background characteristics' effects and the socialisation's effects (Model 2) then all effects together including the structural characteristics' effects (Model 3). This strategy allowed me to isolate the three groups of effects and to detect the critical effects. Specifically, effects that remained significant across the models would be the important ones that could impact the occurrence of InfoSec influence ties, whereas those that lost their impacts on InfoSec influence due to being evaluated with the newly added effects would be considered as weaker effects.

List of specified terms

I specified the three mentioned models by using the latest version 3.6.0 of the statistical package 'ergm' (Hunter et al. 2008), which was implemented in the R programming environment (Hornik 2016). The terms used to model the effects of employees' background characteristics and socialisation and the InfoSec influence network's structural characteristics are summarised in Table D.1.

Table D.1. Terms Included in the Models

Model	Term		Effect
All	edges		This term models the number of directed ties (called 'edges' in ERGM) and its result indicated the likelihood of occurrence of InfoSec influence ties between pairs of random employees in this research context.
Models 1 and 2	nodeocov nodeofactor		These terms model the effect of a nodal characteristic on the occurrence of outgoing InfoSec influence ties. The term *nodeocov* is used to model such effect of numeric variables (e.g., age and tenure), while the term *nodeofactor* is used for categorical/non-numeric variables (e.g., gender and seniority).
	nodeicov nodeifactor		These terms model the effect of a nodal characteristic on the occurrence of incoming InfoSec influence ties. The term *nodeicov* is used to model such effect of numeric variables (e.g., age and tenure), while the term *nodeifactor* is used for categorical/non-numeric variables (e.g., gender and seniority).
	nodematch		These terms model the homophily effect of a nodal characteristic on the occurrence of InfoSec influence ties. Homophily effect means that nodes with similar characteristic will be more likely to establish InfoSec influence ties than nodes with different characteristics. The term *nodematch* is used to model a homophily effect of categorical/non-numeric variables (e.g., gender, seniority and department membership), while the term *absdiff* is used to model such effect of numeric variables (e.g., age and tenure).
	absdiff		
Models 2 and 3	edgecov		This term models the tendency of two types of network ties to co-occur with each other. For example, the likelihood for InfoSec influence ties to co-occur with instrumental/expressive/InfoSec support provision ties.
Model 3	gwodegree		This term models the variation of outgoing ties in the InfoSec influence network. It also models the tendency of active nodes, which have many outgoing ties, to continue sending out more ties.

	gwidegree		This term models the variation of incoming ties in the InfoSec influence network. It also models the tendency of popular nodes, which have many incoming ties, to continue receiving more ties.
	dgwesp		This term models the additional propensity of an InfoSec influence tie between two nodes for each shared partner that they have in common. That is, the tendency of node A to close triads by sending a direct tie to B, given that there are multiple in-between C's that bridge A and B.
	dgwdsp		This term models the two-path pattern between nodes A and B via their shared partners. That is, the tendency of node A to maintain its indirect connections to B via multiple C's in between.
	mutual		This term models the tendency of nodes to reciprocate their ties.
	idegree=0		This term controls for the number of nodes having a zero in-degree in the InfoSec influence network. These nodes are termed 'sources', which refer to the behaviour of only sending ties (out-degree > 0) while not receiving any (in-degree = 0).
	odegree=0		This term controls for the number of nodes having a zero out-degree in the InfoSec influence network. These nodes are termed 'sinks', which refer to the behaviour of only receiving ties (in-degree > 0) while not sending any (out-degree = 0).
	isolates		This term controls for the number of isolates which have zero in-degree and out-degree in the InfoSec influence network.

Source: Morris, Handcock and Hunter (2008).

Model estimation

After specifying the models with the terms which described the formation of InfoSec influence network, the models were analysed by using the Monte Carlo Markov Chain estimation approach with interval and burn-in rates set at 50,000 and 500,000 respectively. Geweke statistics were examined to check for degeneracy during the estimation process. All terms achieved p-values of larger than the statistical significance threshold of 0.05, which indicated that there was no degeneracy (Desmarais & Cranmer 2012). I also compared the Aikake Information Criterion and Bayesian Information Criterion values of the models and Model 3 achieved the best performance, with the lowest score for both of these values.

Goodness-of-fit

Goodness-of-fit for Models 1, 2 and 3 was computed with interval and burn-in rates relatively large at 50,000 and 500,000 to ensure accurate outputs (Goodreau et al. 2008). Figures D.1, D.2 and D.3 visualise the three models' goodness-of-fit evaluated through the distributions of key structural characteristics of the InfoSec influence network, which were in-degree, out-degree, edge-wise shared partners and minimum geodesic distance. The boxplots describe the distributions of the simulated networks' structural statistics generated from the model. The grey lines connect the 95 per cent bounds on the distributions, whereas the solid lines represent the observed network's distributions of the four mentioned structural characteristics.

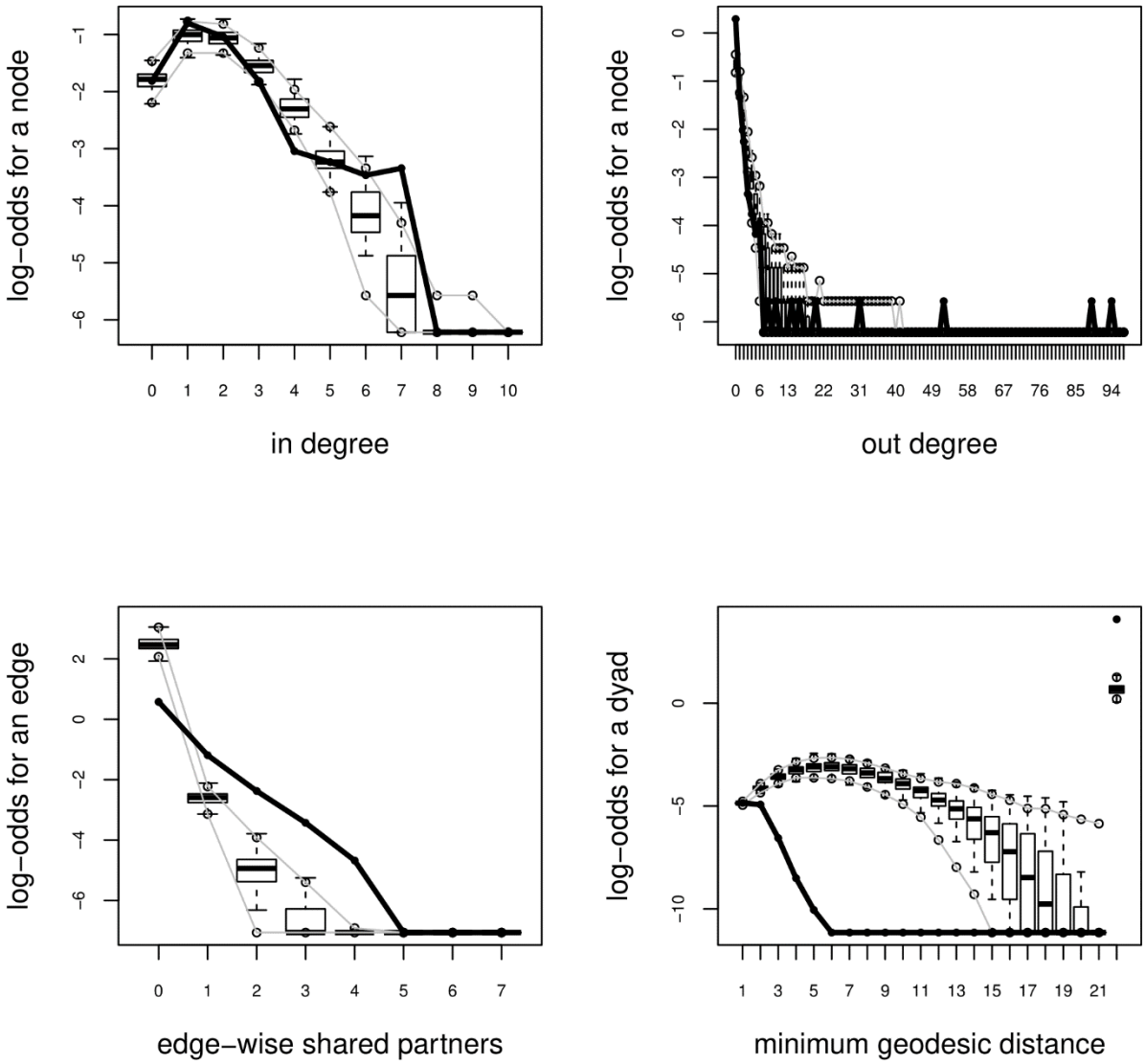


Figure D.1. Goodness-of-Fit of Model 1

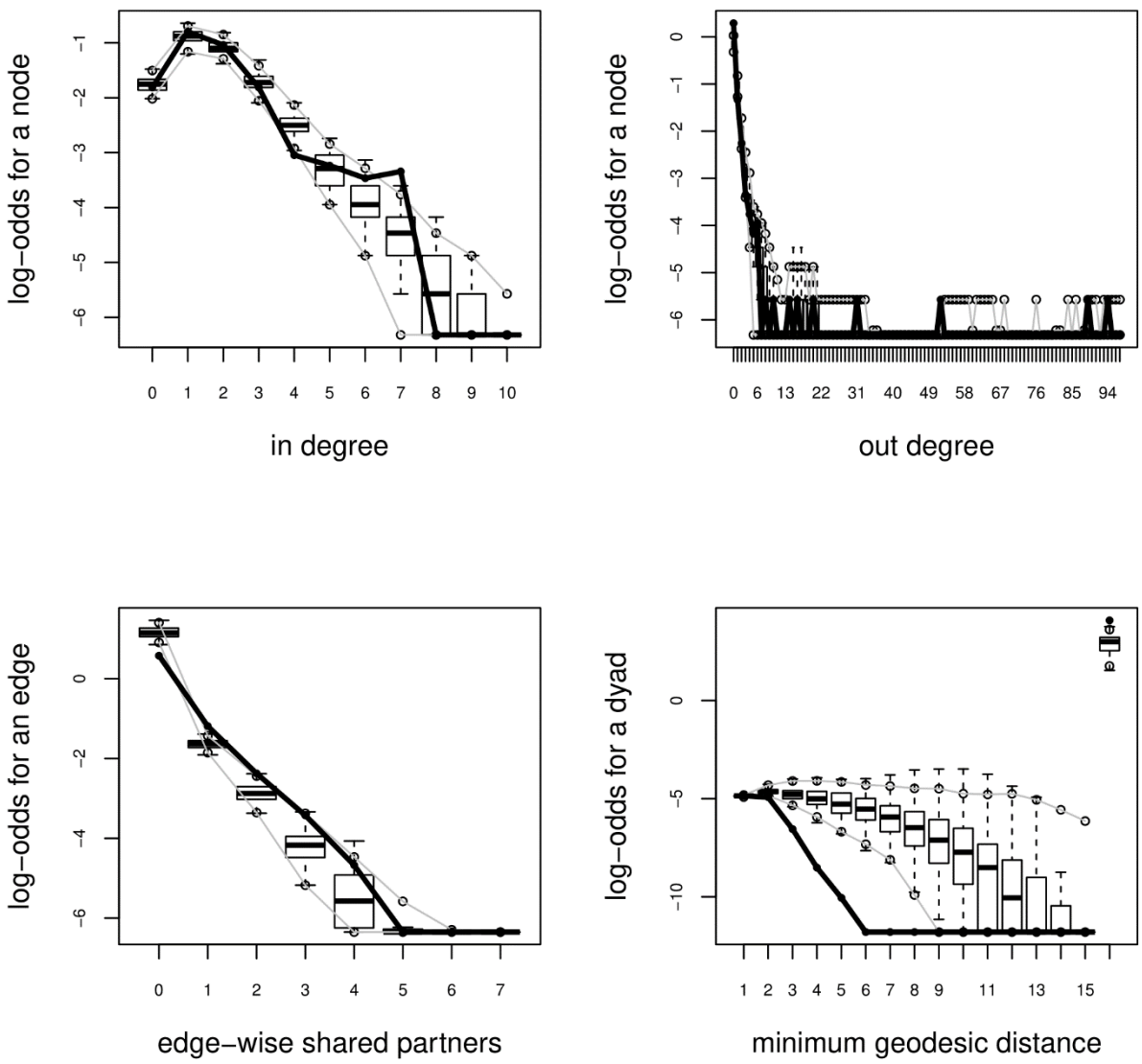


Figure D.2. Goodness-of-Fit of Model 2

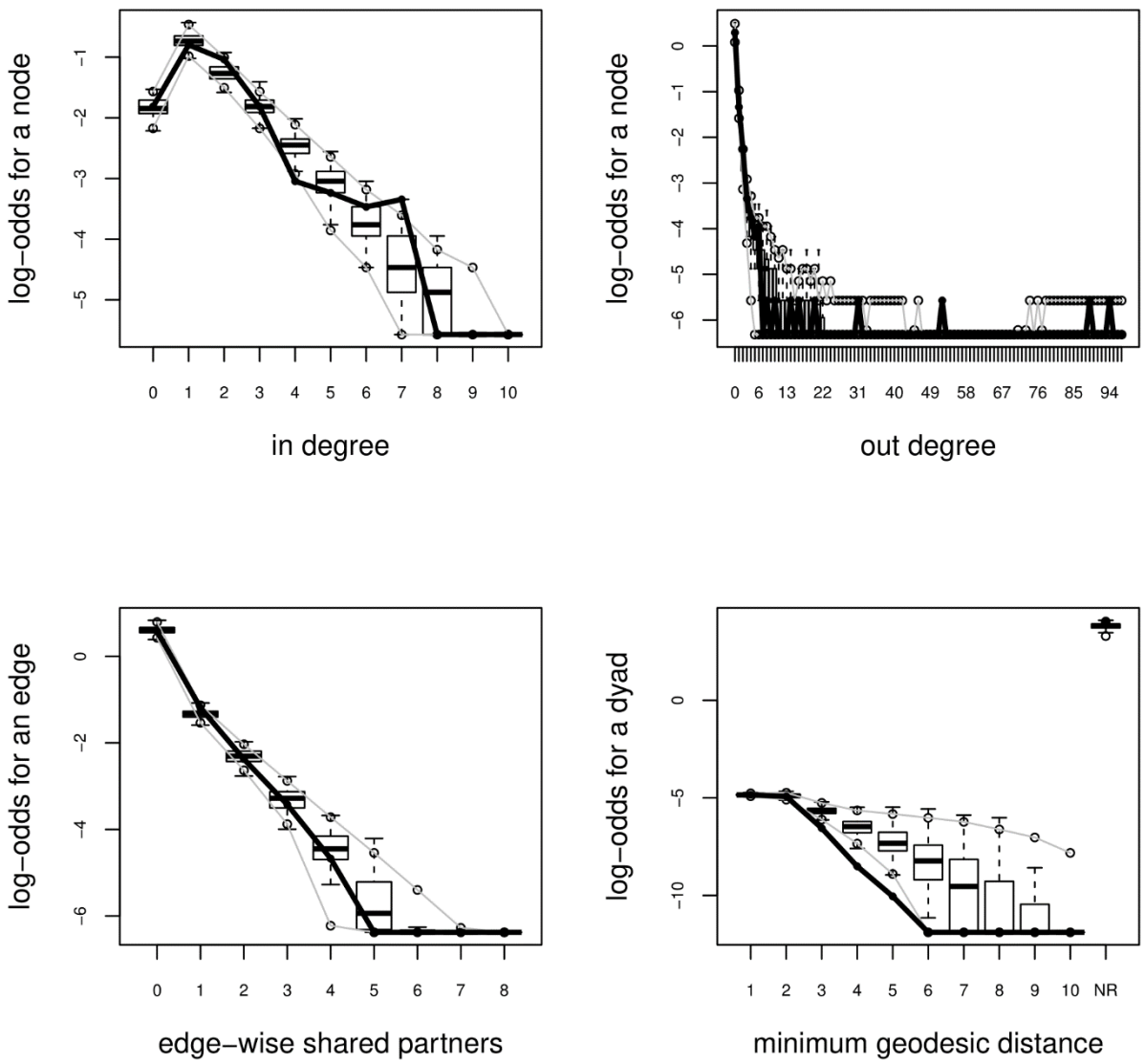


Figure D.3. Goodness-of-Fit of Model 3

Of the three models, Model 3 achieved the best goodness-of-fit, as shown in Figure D.3, where the solid lines ran through the boxplots in the graphs for the in-degree, out-degree and edge-wise shared partners. This indicated that Model 3 described well the InfoSec influence network in terms of its in-degree, out-degree and edge-wise shared partners. Model 3 could not describe well the InfoSec influence network's geodesic distance, but such discrepancy can be overlooked as analysing the network's geodesic distance was not the focus of this stage of the CAR project.

Robustness check

While Figure D.3 showed Model 3's out-degrees and edge-wise shared partners achieved good fit, the goodness-of-fit in regard to the model's in-degrees had some issues. Specifically, the

solid line failed to run through the boxplots which represented the distributions of four, five, six and seven in-degrees. This indicated that Model 3 could not describe well the observed InfoSec influence network's amounts of four, five, six and seven in-degrees.

To ensure that the results of Model 3 were accurate despite the misfits of those in-degrees, I analysed a model named robustness check model based on Model 3 while controlling for the numbers of in-degrees equal to four, five, six and seven. By doing so, I specified this robustness check model to have the same amounts of in-degrees as in the observed network. Then, I compared the results of the robustness check model with Model 3 to check for any discrepancies. The robustness check model was estimated with the same settings (i.e., interval = 50,000; burn-in rates = 500,000) and its goodness-of-fit is shown in Figure D.4.

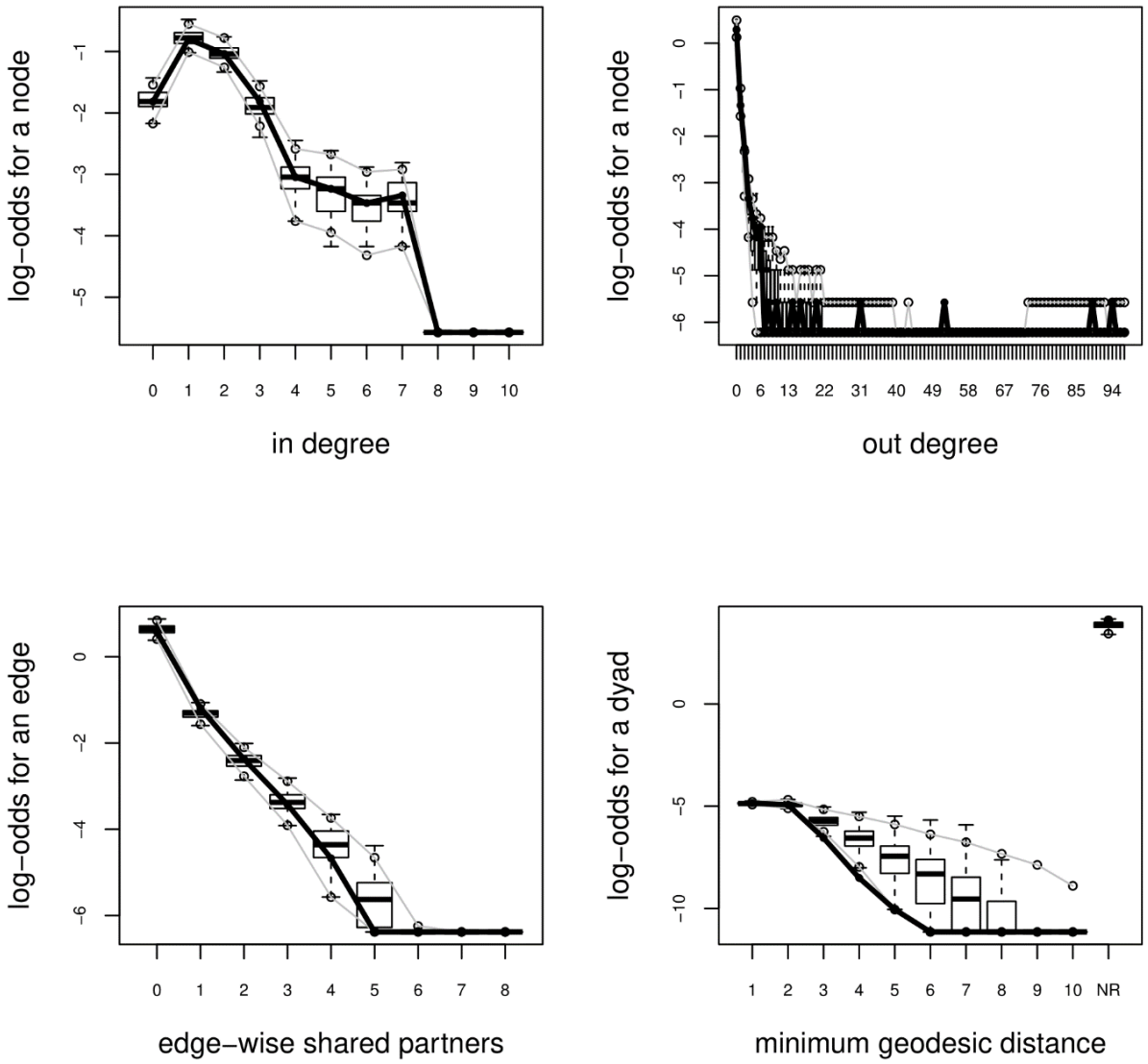


Figure D.4. Goodness-of-Fit of the Robustness Check Model

By controlling for the numbers of in-degrees, the robustness check model's distributions of simulated in-degrees achieved excellent goodness-of-fit (i.e., the solid line ran through all the boxplots in the graph for in-degree). Table D.2 compares the results of Model 3 and the robustness check model. Descriptions of the terms are available in Table D.1.

Table D.2. Comparison of Results of Model 3 and Robustness Check Model

Effect (term in brackets)	Model 3	Robustness check model
Occurrence of InfoSec influence (*edges*)	–4.17	–5.05
Female–influencer (*nodeofactor*)	–0.36	–0.36
Female–influenced (*nodeifactor*)	–0.15	–0.13
Same gender (*nodematch*)	–0.03	–0.03
Same department (*nodematch*)	0.76	0.75
Age–influencer (*nodeocov*)	–0.02	–0.02
Age–influenced (*nodeicov*)	0.01	0.02
Different age (*absdiff*)	–0.01	–0.01
Seniority (*nodematch*)	–0.18	–0.18
Manager–influencer (*nodeofactor*)	0.31	0.32
Director–influencer (*nodeofactor*)	1.35	1.35
Manager–influenced (*nodeifactor*)	–0.03	–0.04
Director–influenced (*nodeifactor*)	0.38	0.39
Tenure–influencer (*nodeocov*)	0.06	0.06
Tenure–influenced (*nodeicov*)	–0.03	–0.03
Different tenure (*absdiff*)	–0.04	–0.04
Instrumental provision (*edgecov*)	1.93	1.93
Expressive provision (*edgecov*)	1.14	1.16
InfoSec support provision (*edgecov*)	4.31	4.3
Out-degree variation (*gwodegree*)	–3.16	–3.18
In-degree variation (*gwidegree*)	–1.03	0.67
Triad closure (*dgwdsp*)	0.5	0.51
Two-path (*dgwesp*)	–0.07	–0.07
Reciprocity (*mutual*)	–1.74	–1.77
Sinks (*out-degree = 0*)	–1.1	–1.11
Sources (*in-degree = 0*)	–0.95	–0.06
Isolated nodes (*isolates*)	–0.19	–0.2
In-degree = 4		–0.07
In-degree = 5		0.95
In-degree = 6		2.1
In-degree = 7		3.45
Akaike Information Criterion	2609	2598
Bayesian Information Criterion	2856	2881

Overall, the two models did not have many discrepancies, except for the terms that described the occurrence of the tie (i.e., 'edges'), in-degrees variation (e.g., 'gwidegree') and the numbers of zero, four, five, six and seven in-degrees. These discrepancies were expected as controlling

for the network's in-degrees made the estimation process adjust results of the terms describing the numbers of in-degrees, which were 'edges', 'gwidegree' and the controls for in-degrees.

The main effects of employees' background characteristics and socialisation on InfoSec influence did not have any large discrepancies in results when controlling for the mentioned numbers of in-degrees. This indicated that, without controlling for in-degrees, Model 3's results could be meaningfully interpreted although its goodness-of-fit was not excellent. In fact, the Bayesian Information Criterion value of Model 3 was lower than that of the robustness check model (see Table D.2). This difference in the Bayesian Information Criterion values suggested that Model 3 was more favourable than the robustness check model. The final results of the three models are summarised in Table D.3.

Table D.3. Results of the Three Models

Effect	Model 1	Model 2	Model 3
Occurrence of InfoSec influence (*edges*)	–2.96*** (0.40)	–4.66*** (0.57)	–4.17*** (0.56)
Female–influencer (*nodeofactor*)	–1.27*** (0.12)	–0.83*** (0.18)	–0.36** (0.15)
Female–influenced (*nodeifactor*)	–0.24** (0.12)	–0.16 (0.16)	–0.15 (0.16)
Same gender (*nodematch*)	0.02 (0.12)	–0.05 (0.16)	–0.03 (0.16)
Same department (*nodematch*)	1.10*** (0.09)	–0.47*** (0.15)	0.76*** (0.15)
Age–influencer (*nodeocov*)	–0.09*** (0.01)	–0.07*** (0.02)	–0.02 (0.01)
Age–influenced (*nodeicov*)	0.001 (0.01)	0.02 (0.01)	0.01 (0.01)
Different age (*absdiff*)	–0.01 (0.01)	–0.02 (0.01)	–0.01 (0.01)
Seniority (*nodematch*)	0.06 (0.13)	–0.27 (0.18)	–0.18 (0.19)
Manager–influencer (*nodeofactor*)	1.48*** (0.15)	0.72*** (0.20)	0.31 (0.19)
Director–influencer (*nodeofactor*)	1.51*** (0.41)	1.88*** (0.46)	1.35*** (0.30)
Manager–influenced (*nodeifactor*)	0.30** (0.14)	–0.03 (0.19)	–0.03 (0.19)
Director–influenced (*nodeifactor*)	0.54 (0.47)	0.24 (0.64)	0.38 (0.61)
Tenure–influencer (*nodeocov*)	0.23*** (0.02)	0.16*** (0.02)	0.06*** (0.02)
Tenure–influenced (*nodeicov*)	–0.01 (0.01)	–0.03 (0.02)	–0.03** (0.02)
Different tenure (*absdiff*)	–0.08*** (0.01)	–0.05*** (0.02)	–0.04** (0.02)
Instrumental provision (*edgecov*)		1.98*** (0.21)	1.93*** (0.19)
Expressive provision (*edgecov*)		0.91*** (0.22)	1.14*** (0.21)
InfoSec support provision (*edgecov*)		5.33*** (0.12)	4.31*** (0.14)
Out-degree variation (*gwodegree*)			–3.16*** (0.39)
In-degree variation (*gwidegree*)			–1.03*** (0.38)
Triad closure (*dgwdsp*)			0.50*** (0.10)
Two-path (*dgwesp*)			–0.07*** (0.03)
Reciprocity (*mutual*)			–1.74 (1.19)
Sinks (*out-degree = 0*)			–1.10*** (0.39)
Sources (*in-degree = 0*)			–0.95** (0.44)
Isolated nodes (*isolates*)			–0.19 (0.39)
Akaike Information Criterion	5438	2763	2609
Bayesian Information Criterion	5584	2937	2856

Note: **p < 0.05; ***p < 0.01.

Table D.4. List of InfoSec Champions

ID	Department	Gender	Age	Tenure	Seniority	INS_Outdeg	EXP_Outdeg	ISS_Outdeg	INF_Outdeg	INS_Beta	EXP_Beta	ISS_Beta	INF_Beta
1	Accounting	Female	40	11	Staff	5	3	0	1	13.6	342.3	0.0	1.0
2	Accounting	Female	50	16	Staff	5	4	0	2	10.6	162.2	0.0	400.0
3	Administration	Female	32	8	Manager	27	7	2	5	3647.2	1380.6	7.9	17.9
4	Administration	Female	32	7	Staff	15	7	2	1	1610.6	871.4	4.0	3.0
5	Architect	Female	35	1	Manager	3	3	0	1	376.6	312.8	0.0	1.0
6	Architect	Male	30	0	Staff	1	1	3	0	1.0	1.0	4.0	0.0
7	Architect	Male	31	5	Staff	2	8	5	2	2.7	4644.7	7.0	2.0
8	Architect	Male	30	1	Staff	1	5	0	0	1734.1	1561.9	0.0	0.0
9	Architect	Female	39	13	Staff	1	4	0	0	1.7	3017.3	0.0	0.0
10	Architect	Female	32	7	Manager	22	11	6	8	6111.6	3661.1	2093.8	11.0
11	Architect	Female	34	9	Staff	3	2	0	0	1317.6	1338.4	0.0	0.0
12	Architect	Male	37	16	Manager	3	0	1	0	823.6	0.0	1.0	0.0
13	Architect	Female	26	2	Staff	2	6	0	0	2.8	1773.2	0.0	0.0
14	Architect	Male	36	14	Manager	12	17	5	6	1707.0	10224.0	2091.3	6.0
15	ASS	Female	28	0	Staff	7	3	5	5	15.1	132.5	12.0	16.9
16	BSP	Female	34	4	Manager	0	0	5	2	0.0	0.0	803.5	5.0
17	BSP	Male	30	0	Staff	1	1	1	0	1.7	1.3	2.0	0.0
18	BusDev	Female	29	1	Staff	4	6	4	0	9.3	1001.7	14.9	0.0
19	Construction	Male	42	14	Manager	19	6	1	3	56.3	930.6	790.6	5.0
20	Construction	Female	43	20	Manager	16	10	3	4	2179.3	6814.7	4.0	309.7
21	Construction	Male	31	7	Staff	2	7	0	2	2.0	729.7	0.0	2.0
22	Construction	Male	33	12	Staff	10	10	3	6	19.5	1409.1	3.0	303.8
23	Construction	Female	38	1	Staff	16	4	9	6	31.5	126.4	1595.1	305.2
24	Construction	Female	26	1	Staff	16	7	5	5	22.6	217.6	2384.6	902.2
25	Estimation	Male	29	2	Staff	2	3	1	1	2.5	469.1	3.0	1.0

26	Estimation	Female	29	7	Manager	8	10	2	5	604.8	1941.9	9.9	1000.0
27	Factory	Male	26	4	Staff	1	2	9	4	1.6	7.7	17.9	5.0
28	Factory	Male	50	15	Manager	10	9	24	20	14.7	65.1	46.8	435.9
29	Factory	Male	39	14	Staff	0	3	5	4	0.0	11.4	13.9	5.0
30	Factory	Female	37	8	Manager	5	7	0	1	8.2	75.3	0.0	1.0
31	Factory	Male	36	7	Manager	10	6	7	4	19.7	47.8	19.9	403.0
32	Factory	Female	31	6	Staff	4	5	2	2	5.6	23.6	3.0	3.0
33	Gamma	Male	33	2	Director	1	1	1	1	1.7	69.9	200.0	2.0
34	Gamma	Female	35	1	Manager	2	1	1	1	2.5	16.1	200.0	1.0
35	Hanoi	Female	34	3	Manager	0	0	0	0	0.0	0.0	0.0	0.0
36	HR	Female	31	4	Staff	20	7	2	1	7979.0	1243.1	3.0	1.0
37	HR	Male	38	7	Manager	42	3	1	2	10846.8	318.1	2.0	4.0
38	Marketing	Female	37	0	Manager	3	3	0	0	1101.8	179.9	0.0	0.0
39	Marketing	Male	34	9	Manager	7	3	2	2	3857.5	520.9	2.0	2.0
40	PM	Female	36	2	Staff	7	8	2	1	9.3	968.4	1584.1	1.0
41	PM	Female	32	11	Manager	33	11	6	10	3910.8	860.1	3167.2	309.7
42	PM	Female	32	4	Staff	12	6	1	1	32.2	1192.9	4.0	1.0
43	PM	Female	25	2	Staff	2	5	3	1	2.0	342.2	3.0	2.0
44	PM	Female	31	2	Staff	4	5	3	1	5.9	1067.9	5.0	1.0
45	Purchasing	Female	33	1	Manager	2	2	1	1	4.1	2.0	1.0	1.0
46	Purchasing	Female	39	3	Staff	3	7	1	1	12.6	1606.3	1.0	1.0
47	Purchasing	Female	30	3	Manager	6	8	2	0	12.8	1360.7	6.0	0.0
48	QC	Female	34	1	Manager	1	2	0	0	1.0	219.0	0.0	0.0
49	Tender	Female	33	10	Staff	4	3	1	1	16.0	657.5	3.0	2.0
50	Tender	Female	30	2	Staff	4	5	2	1	14.8	911.3	7.0	2.0

Notes: INS = Instrumental network; EXP = Expressive network; ISS = InfoSec support network; INF = InfoSec influence network; Outdeg = out-degree centrality (i.e., the number of nodes that a node sends ties to); Beta = Beta centrality (i.e., the indirect popularity of a node based on its well-connected neighbours).

Appendix E. Computing Single-Item InfoSec Climate Scores

SAOM and its tool RSiena required variables that represented nodal attributes (e.g., behaviours and perceptions) to be single items that have integer values (Ripley et al. 2017). As such, the latent constructs about employees' climate perceptions of colleagues' and direct supervisors' InfoSec behaviours had to be converted into the required data format.

Rather than averaging the items that represented employees' climate perceptions (see Table 6.2 in Chapter 6), I performed confirmatory factor analysis (Brown 2006) to accurately calculate the single-item scores for each employee that represented their climate perceptions. While the averaging method assumes that every item has an equal amount of contribution towards the resulting single-item variable, the confirmatory factor analysis method estimates the exact amount of loading of each measurement item as part of the latent construct (i.e., perception of InfoSec climate). As a result, I could determine which items contributed the most to the construct and accurately calculate the construct's score for each respondent.

I performed confirmatory factor analysis by using the software AMOS version 20 (Arbuckle 2011) which specified the relationships between the measurement items collected by using the questions listed in Table 6.2 and perceptions of InfoSec climate. The measurement models for each construct (i.e., perception of colleagues' InfoSec behaviours and perception of direct supervisors' InfoSec behaviours) were specified and evaluated separately. Both models were specified and evaluated under the assumption that the respondent's perception before the InfoSec change program affects their perception after the program. The specification of this assumption is realistic and another advantage of using confirmatory factor analysis method, compared to averaging the items to calculate the single-item scores for each time point while ignoring their interdependency.

The measurement models are illustrated in Figures E.1 and E.2. The oval objects represented the latent constructs which were climate perceptions of colleagues' and direct supervisors' InfoSec behaviours at Time 1 (i.e., before the change program) and Time 2 (i.e., after the change program). The square objects represented the measurement items or the respondents' answers for the survey questions. The arrows from the latent constructs to the measurement items denoted that the unobservable latent constructs were reflected by the observable measurement items. The circle objects with a letter 'e' were the unobservable errors that

associated with each measurement item which represented measurement errors. The curved arrows between the measurement errors denoted their correlations between the two points in time.

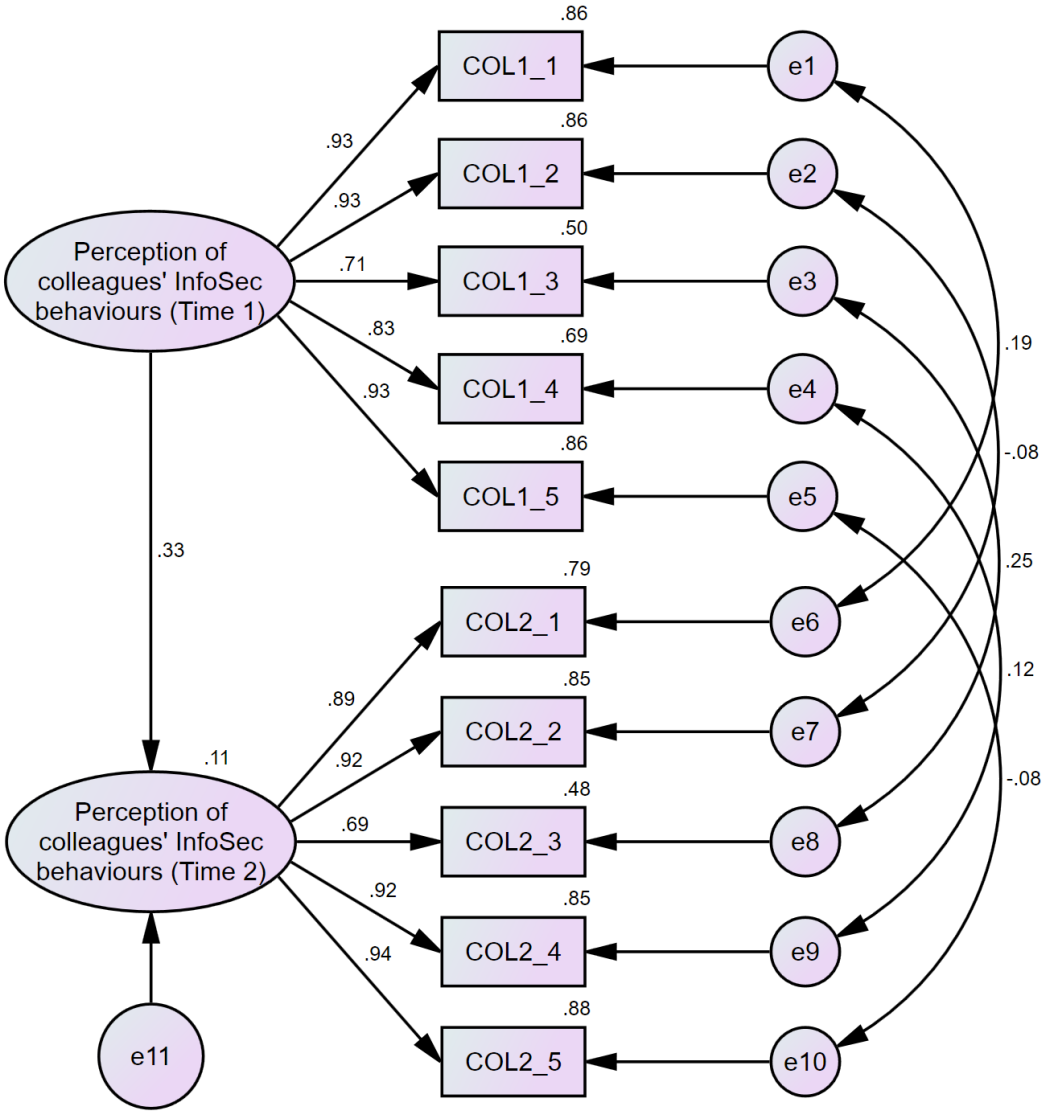


Figure E.1. Measurement Model of Perception of Colleagues' InfoSec Behaviours

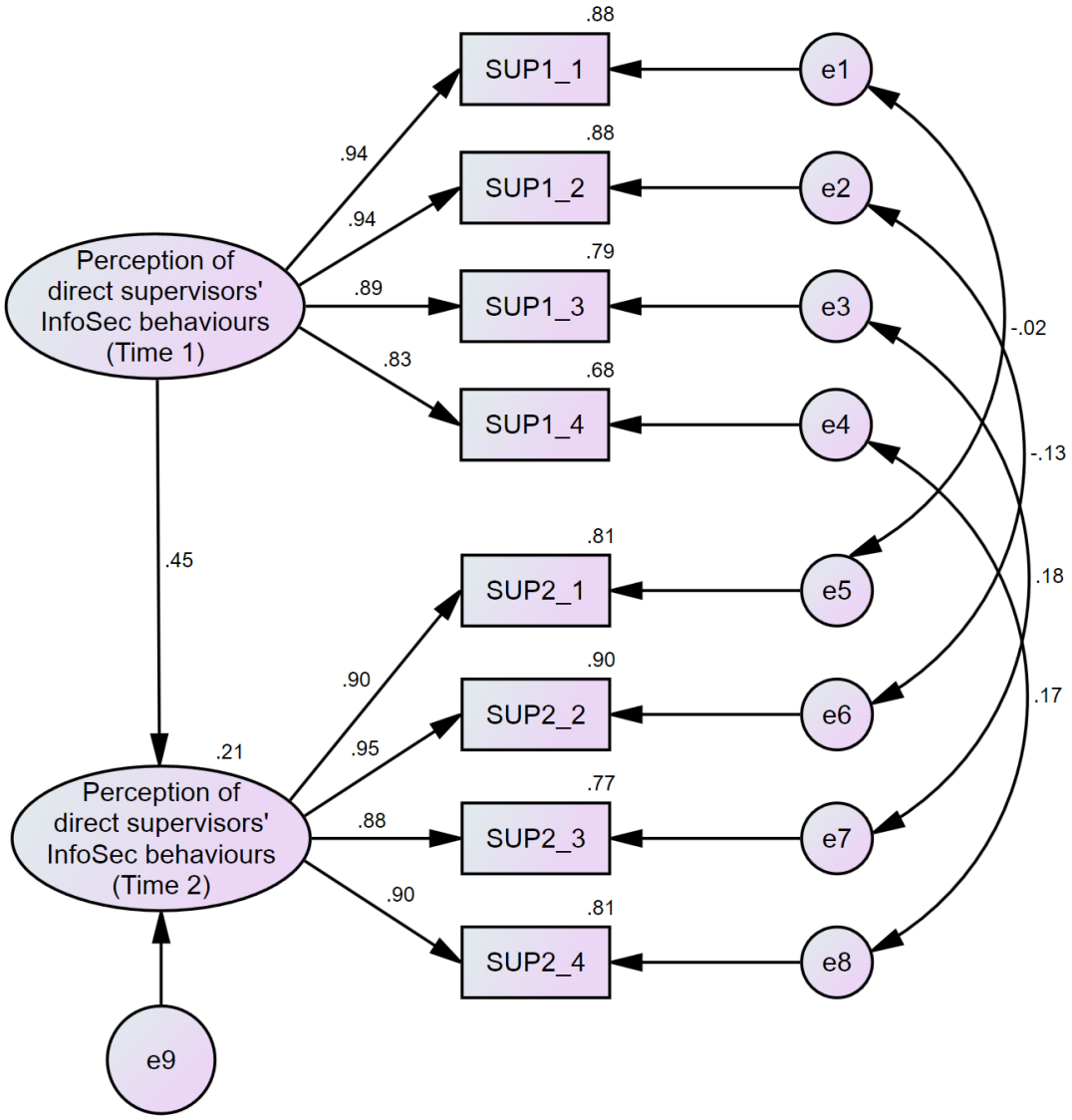


Figure E.2. Measurement Model of Perception of Direct Supervisors' InfoSec Behaviours

A challenge when specifying the measurement models was that the collected data violated the multivariate normality assumption, and this rendered the default estimation method in AMOS called Maximum Likelihood (Byrne 2010) inappropriate and demanded the use of Bollen–Stine bootstrapping method (Bollen & Stine 1992). After specifying and evaluating the models for perceptions of colleagues' and direct supervisors' InfoSec behaviours, I found that both models exhibited acceptable goodness-of-fit with Bollen–Stine bootstrap with p-values equal to 0.343 and 0.653 respectively. This meant that the specified structures and measurements of the climate perceptions adequately reflected the observed data.

Table E.1 show that there were no issues with convergent validity, except the removal of item SUP5 from the model due to its factor loadings of –0.12 and 0.08 for Time 1 and Time 2

respectively, which were much lower than the recommended threshold of ±0.35 (Lewis, Templeton & Byrd 2005). Reliability of the constructs was assessed by calculating both Cronbach's alpha and coefficient H. The common use of Cronbach's alpha is prone to inaccurate evaluation of reliability, especially in this project as this index assumes the measurement model to be essentially tau-equivalent (i.e., all item's loadings are specified to have equal values) (Graham 2006). However, I did not specify the measurement models in such a way. In this context, the coefficient H provides a more accurate evaluation of reliability (Hancock & Mueller 2001).

Table E.1. Convergent Validity

Construct	Item	Time 1			Time 2		
		Loading	α	H	Loading	α	H
Climate perception of direct supervisors' InfoSec behaviours (SUP)	SUP1	0.94	0.94	0.95	0.90	0.95	0.95
	SUP2	0.94			0.95		
	SUP3	0.89			0.88		
	SUP4	0.83			0.90		
	SUP5	Dropped			Dropped		
Climate perception of colleagues' InfoSec behaviours (COL)	COL1	0.93	0.94	0.96	0.89	0.94	0.96
	COL2	0.93			0.92		
	COL3	0.71			0.69		
	COL4	0.83			0.92		
	COL5	0.93			0.94		
Acceptable criteria		> ±0.35	> 0.70	> 0.70	> ±0.35	> 0.70	> 0.70

Once the factor score weights of the measurement items were computed from the measurement model (see Table E.2), I multiplied these factor score weights with the answers provided by the respondents to the measurement items (i.e., SUP 1–4 and COL 1–5) then added them together. This calculation created two single-item scores per respondent, which represented the respondent's climate perceptions of colleagues and direct supervisors' InfoSec behaviours before and after the change program.

Table E.2. Items' Factor Scores of Climate Perceptions at Time 1 (pre-change program) and Time 2 (post-change program)

	COL1_1	COL1_2	COL1_3	COL1_4	COL1_5	COL2_1	COL2_2	COL2_3	COL2_4	COL2_5
COL (Time 1)	0.236	0.231	0.044	0.08	0.231	-0.035	0.031	-0.011	-0.08	0.032
COL (Time 2)	-0.021	0.022	-0.007	-0.01	0.024	0.134	0.195	0.039	0.178	0.221
	SUP1_1	**SUP1_2**	**SUP1_3**	**SUP1_4**	**SUP1_5**	**SUP2_1**	**SUP2_2**	**SUP2_3**	**SUP2_4**	**SUP2_5**
SUP (Time 1)	0.29	0.296	0.155	0.099	Dropped	0.01	0.055	-0.027	-0.02	Dropped
SUP (Time 2)	0.012	0.048	-0.022	-0.02	Dropped	0.17	0.348	0.156	0.193	Dropped

I demonstrate the calculation of the climate perceptions' scores as follows. Let us assume that there was an employee A with their responses for the questions about direct supervisors' InfoSec behaviours summarised in Table E.3.

Table E.3. Sample Answers for Questions about Climate Perception of Direct Supervisors' InfoSec Behaviours

	Time 1				Time 2			
	SUP1_1	**SUP1_2**	**SUP1_3**	**SUP1_4**	**SUP2_1**	**SUP2_2**	**SUP2_3**	**SUP2_4**
Employee A's answers	4	5	5	4	7	6	7	6

Following the described procedure, the score of employee A's climate perception of direct supervisors before the change program is calculated by summing the products of employee A's answers (see Table E.3) and the factor score weights listed in the fifth row of Table E.2:

$$\begin{aligned} &Employee\ A's\ climate\ perception\ score\ (Time\ 1) \\ &\quad = (0.29 \times 4 + 0.296 \times 5 + 0.155 \times 5 + 0.099 \times 4) \\ &\quad + (0.01 \times 7 + 0.055 \times 6 - 0.027 \times 7 - 0.02 \times 6) = 4\ (rounded) \end{aligned}$$

Similarly, employee's A climate perception score after the change program is calculated by summing the products of employee A's answers and the factor score weights listed in the sixth row of Table E.2:

$$\begin{aligned} &Employee\ A's\ climate\ perception\ score\ (Time\ 2) \\ &\quad = (0.012 \times 4 + 0.048 \times 5 - 0.022 \times 5 - 0.02 \times 4) \\ &\quad + (0.17 \times 7 + 0.348 \times 6 + 0.156 \times 7 + 0.193 \times 6) = 6\ (rounded) \end{aligned}$$

The scores were then rounded to the nearest integer to satisfy SAOM's requirement for data (Ripley et al. 2017).

Appendix F. Stochastic Actor-Oriented Modelling Process

The specification of a SAO model to achieve acceptable goodness-of-fit can be described as a trial-and-error process where researchers began with including terms that correspond to the theoretical model, then evaluate the model's goodness-of-fit and add terms about the structural mechanisms of the network to improve goodness-of-fit if needed. Another reason for such a trial-and-error approach is due to the various effects of social influence that can be modelled, which include the assimilation and contagion effects (Steglich, Snijders & Pearson 2010).

During the SAOM process, researchers can decide whether one or more terms should be tested with the Wald or score-type tests. Wald tests, which include the use of t-test to determine a parameter's statistical significance, can be performed easily by dividing the produced estimate by its standard error (Ripley et al. 2017). However, there are cases where the results may arrive at unusually large estimates and/or standard errors, which make the use of t-test inappropriate. In these cases, researchers are recommended to test the results by using the score test (Ripley et al. 2017). This score test allows the researchers to fix the problematic parameters to a constant (i.e., usually zero, which establishes the null hypothesis that the parameter does not have any effect) and test the fixed parameters without estimating them.

The evaluation of a SAO model focuses on three features, 1) the convergence of each term and the model, 2) goodness-of-fit and 3) any abnormalities in the produced estimates and standard errors. Ripley et al. (2017) recommended that published SAOM results should achieve a maximum convergence ratio for the whole model that is less than 0.25, while the convergence t-ratio that describes convergence of each modelled term should be less than 0.1.

All SAO models in the evaluation and reflection stage of this CAR project were estimated with stringent settings for the estimation method to produce reliable results. I set the number of sub-phases at six (instead of four by default) to increase precision and the number of runs in the final phase 3 of the estimation at 5000 to increase reliability (instead of 1,000 by default) (Ripley et al. 2017).

Contagion models

In line with the modelling strategy (see Section 8.3.3), I started with analysing the SAO model that incorporated the weighted average contagion effect. This effect described the phenomenon where employees increased their climate perception scores as they received InfoSec influence

from their colleagues in the same department, whose climate perception scores were high. It was worth highlighting that the weighted average contagion effect assumed that all employees experienced the same contagion effect regardless of how many InfoSec influencers they had. Since there were two types of climate perceptions (i.e., perceptions of co-workers and direct supervisors' InfoSec behaviours), the same weighted average contagion effect was modelled for each of them. Moreover, I included employees' background characteristics as control variables assumed to impact the climate perceptions.

The model's maximum convergence ratio was 0.1209, lower than the recommended threshold of 0.25 (Ripley et al. 2017). Moreover, every included term's convergence t-ratio was lower than the recommended threshold of 0.1 (Ripley et al. 2017). These results indicated that the model converged well and its results were reliable for interpretation. The estimates and standard errors were reasonably small, which indicated that there were no issues with the results.

Table F.1 summarises the results of the weighted average contagion model. The effects associated with the climate perception scores of colleagues' InfoSec behaviours and direct supervisors' InfoSec behaviours are presented separately in the table. Statistical significance was determined by using the t-test (i.e., divide the estimate by the standard error and check whether the result is larger than or equal to 1.96) (Ripley et al. 2017). The significance of the rate effects was not necessarily evaluated and reported as the changes in the InfoSec influence network before and after the change program (see Section 8.3.7) already suggested that the rate effect would be positive (Ripley et al. 2017).

The estimates presented in all SAO models were in log-odds ratios and could be interpreted as follows. The estimate of the champion alter effect was 0.44, which described the likelihood that an employee would receive InfoSec influence from another employee who held the champion role. By taking the exponential of this estimate (i.e., $e^{0.44}$), the effect can be interpreted that the likelihood for a champion to exert InfoSec influence over an employee was 1.56 times higher than that for a non-champion. With regard to the weighted average contagion effect, the model did not detect employees' tendency towards higher scores of both types of climate perceptions as caused by receiving InfoSec influence from colleagues with high climate perceptions' scores in the same department. This was due to the weighted average contagion effects were not significant (i.e., ratio of estimate and standard error was smaller than 1.96).

Table F.1. Results of Weighted Average Contagion Model

Dynamics of InfoSec influence network	Estimate (Std. Error)	Converg. t-ratio
Rate of InfoSec influence	8.95 (2.51)	–0.01
Out-degree (likelihood of exerting InfoSec influence)	–7.63*** (0.62)	-0.02
Reciprocity	–0.7 (0.59)	<0.01
Transitivity (GWESP I -> K -> J)	1.86*** (0.94)	<0.01
In-degree popularity	1.76*** (0.26)	–0.01
Out-degree activity	0.9*** (0.22)	–0.02
Out-in degree assortativity	–0.3*** (0.1)	0.01
Structural equivalence (in terms of in-degree)	0.11*** (0.02)	<0.01
Exerting InfoSec influence between employees in the same department	1.32*** (0.17)	0.02
Female employees exerted InfoSec influence	–0.08 (0.15)	–0.02
Female employees received InfoSec influence	–0.15 (0.18)	<0.01
Exerting InfoSec influence between employees of the same gender	0.14 (0.14)	<0.01
Old employees exerted InfoSec influence	–0.01 (0.01)	–0.02
Old employees received InfoSec influence	<0.01 (0.01)	<0.01
Exerting InfoSec influence between employees of similar age	–0.55 (0.5)	–0.01
Employees with long tenure exerted InfoSec influence	0.01 (0.02)	<0.01
Employees with long tenure received InfoSec influence	0.01 (0.02)	–0.01
Exerting InfoSec influence between employees of similar tenure	0.39 (0.4)	–0.01
Employees with high seniority exerted InfoSec influence	0.1 (0.24)	–0.03
Employees with high seniority received InfoSec influence	0.01 (0.26)	–0.01
Exerting InfoSec influence between employees with the same seniority	–0.05 (0.25)	0.01
Employees with champion status exerted InfoSec influence	0.44*** (0.13)	0.01
Exerting InfoSec influence between employees with similar CIB	1.2 (1.77)	0.03
Exerting InfoSec influence between employees with similar DSIB	–1.18 (0.91)	–0.01
Provision of work advice and/or organisational updates	1.43*** (0.32)	0.02
Provision of personal advice and/or trust in expertise	1.47*** (0.3)	0.03
Provision of InfoSec advice and/or troubleshooting support	0.99*** (0.33)	–0.01
Dynamics of climate perceptions of CIB	**Estimate (Std. Error)**	**Converg. t-ratio**
Rate of perception of CIB	2.01 (0.44)	–0.01
Linear shape of perception of CIB	0.02 (0.16)	–0.03
Quadratic shape of perception of CIB	–0.97*** (0.44)	–0.01
Average contagion by InfoSec influence of same department employees	0.84 (1.52)	<0.01
Effect of gender (female) on perception of CIB	–0.01 (0.33)	<0.01

Effect of age on perception of CIB	–0.03 (0.03)	<0.01
Effect of tenure on perception of CIB	–0.03 (0.04)	–0.01
Effect of seniority on perception of CIB	–0.13 (0.39)	<0.01
Effect of champion status on perception of CIB	–0.68 (0.43)	0.01
Dynamics of climate perceptions of DSIB	**Estimate (Std. Error)**	**Converg. t-ratio**
Rate of perception of DSIB	2.83 (0.54)	<0.01
Linear shape of perception of DSIB	0.65*** (0.24)	0.01
Quadratic shape of perception of DSIB	–0.42*** (0.11)	-0.01
Average contagion by InfoSec influence of same department employees	–0.08 (0.69)	0.03
Effect of gender (female) on perception of DSIB	–0.19 (0.23)	0.01
Effect of age on perception of DSIB	–0.03 (0.02)	0.02
Effect of tenure on perception of DSIB	<0.01 (0.02)	0.02
Effect of seniority on perception of DSIB	–0.16 (0.26)	0.03
Effect of champion status on perception of DSIB	–0.08 (0.25)	0.02

Note: *** denotes statistical significance; CIB = colleagues' InfoSec behaviours; DSIB = direct supervisors' InfoSec behaviours.

Since the weighted average contagion effect in Table F.1 did not account for the number of InfoSec influencers who exerted InfoSec influence over employees, I accounted for the total number of connections and estimated the model again by using the weighted total contagion effect for the next model.

This model converged well with a maximum convergence ratio of 0.1258 and all terms achieved convergence t-ratios that were lower than 0.01. Table F.2 summarises the results of the weighted total contagion model. All estimates and standard errors were reasonably small, except for the weighted total contagion effect on climate perception of colleagues' InfoSec behaviours. The standard error of this effect was rather large (23.41). While all effects had the same statistical significance and similar estimates as those of the weighted average contagion model, the quadratic shape effect of the weighted total contagion model was not significant. I suspected that such a difference might associate with the unusually large standard error of the weighted total contagion effect.

Table F.2. Results of Weighted Total Contagion Model

Dynamics of InfoSec influence network	Estimate (Std. Error)	Converg. t-ratio
Rate of InfoSec influence	8.88*** (2.57)	–0.03
Out-degree (likelihood of exerting InfoSec influence)	–7.69*** (0.71)	–0.01
Reciprocity	–0.7 (0.71)	–0.01
Transitivity (GWESP I -> K -> J)	1.88 (1.01)	–0.03
In-degree popularity	1.77*** (0.23)	–0.03
Out-degree activity	0.93*** (0.23)	–0.01
Out-in degree assortativity	–0.31*** (0.1)	–0.03
Structural equivalence (in terms of in-degree)	0.11*** (0.02)	0.04
Exerting InfoSec influence between employees in the same department	1.32*** (0.19)	<0.01
Female employees exerted InfoSec influence	–0.09 (0.15)	0.02
Female employees received InfoSec influence	–0.15 (0.18)	<0.01
Exerting InfoSec influence between employees of the same gender	0.14 (0.14)	–0.01
Old employees exerted InfoSec influence	–0.01 (0.01)	0.02
Old employees received InfoSec influence	<0.01 (0.01)	–0.02
Exerting InfoSec influence between employees of similar age	–0.58 (0.54)	–0.02
Employees with long tenure exerted InfoSec influence	<0.01 (0.02)	–0.01
Employees with long tenure received InfoSec influence	0.01 (0.02)	–0.03
Exerting InfoSec influence between employees of similar tenure	0.39 (0.42)	<0.01
Employees with high seniority exerted InfoSec influence	0.09 (0.28)	–0.01
Employees with high seniority received InfoSec influence	–0.01 (0.35)	–0.03
Exerting InfoSec influence between employees with the same seniority	–0.06 (0.33)	–0.01
Employees with champion status exerted InfoSec influence	0.44*** (0.16)	<0.01
Exerting InfoSec influence between employees with similar CIB	1.31 (1.85)	–0.02
Exerting InfoSec influence between employees with similar DSIB	–1.24 (0.92)	<0.01
Provision of work advice and/or organisational updates	1.43*** (0.32)	0.02
Provision of personal advice and/or trust in expertise	1.47*** (0.32)	0.01
Provision of InfoSec advice and/or troubleshooting support	0.99*** (0.3)	–0.01
Dynamics of climate perceptions of CIB	**Estimate (Std. Error)**	**Converg. t-ratio**
Rate of perception of CIB	1.95*** (0.38)	–0.03
Linear shape of perception of CIB	0.78 (2.53)	0.01
Quadratic shape of perception of CIB	–2.8 (7.56)	–0.03
Total contagion by InfoSec influence of same department employees	5.99 (23.41)	<0.01
Effect of gender (female) on perception of CIB	–0.23 (0.84)	<0.01

Effect of age on perception of CIB	–0.07 (0.2)	-0.02
Effect of tenure on perception of CIB	–0.07 (0.18)	-0.01
Effect of seniority on perception of CIB	–0.55 (1.18)	0.01
Effect of champion status on perception of CIB	–1.74 (4.36)	0.01
Dynamics of climate perceptions of DSIB	**Estimate (Std. Error)**	**Converg. t-ratio**
Rate of perception of DSIB	2.83*** (0.62)	<0.01
Linear shape of perception of DSIB	0.63*** (0.2)	0.01
Quadratic shape of perception of DSIB	–0.41*** (0.11)	0.01
Total contagion by InfoSec influence of same department employees	–0.03 (0.48)	–0.01
Effect of gender (female) on perception of DSIB	–0.19 (0.22)	–0.02
Effect of age on perception of DSIB	–0.03 (0.02)	<0.01
Effect of tenure on perception of DSIB	<0.01 (0.03)	0.01
Effect of seniority on perception of DSIB	–0.16 (0.25)	0.02
Effect of champion status on perception of DSIB	–0.09 (0.24)	<0.01

Note: *** denotes statistical significance; CIB = colleagues' InfoSec behaviours; DSIB = direct supervisors' InfoSec behaviours.

Ripley et al. (2017) postulate that when an estimate has an unusually large standard error while the model converged well, then the estimate can still be used but not the standard error. They further advise that researchers in this case can estimate the model several times and check the stability of the estimate and standard error of the problematic term. I estimated the weighted total contagion model three times and detected stability in both statistics, which indicated that I could continue interpreting the current estimate of the weighted total contagion effect for climate perception of colleagues InfoSec behaviours (i.e., a positive value of 5.99), while ignoring its large standard error of 23.41. Ripley et al. (2017) also recommend using the score test on the problematic effect. I proceeded with the score test on the weighted total contagion effects. The score-tested results are summarised in Table F.3.

Table F.3. Score Test Results for the Weighted Total Contagion Effects

Effect	Chi-squared	p-value	One-sided normal variate	One-step estimate
Total contagion by InfoSec influence of same department employees (perception of CIB)	9.42	<0.01	3.07	2.09
Total contagion by InfoSec influence of same department employees (perception of DSIB)	< 0.01	0.95	–0.06	–0.08

Note: CIB = colleagues' InfoSec behaviours; DSIB = direct supervisors' InfoSec behaviours.

The weighted total contagion effect on climate perception of co-workers' InfoSec behaviours achieved statistical significance (Chi-squared = 9.42; p-value < 0.01), whereas the weighted total contagion effect on climate perception of direct supervisors' InfoSec behaviours was not significant. The values of both one-sided normal variate and one-step estimate were positive, 3.07 and 2.09 respectively, which indicated that the weighted total contagion effect on climate perception of co-workers' InfoSec behaviours had positive value (Lomi et al. 2011; Ripley et al. 2017). The quadratic shape effect also became significant when the score test for the weighted total contagion effect was performed, which was consistent with the weighted average contagion model (see Table F.1).

Overall, these results in Tables F.1 and F.3 suggested that the more employees received InfoSec influence from colleagues in the same department whose climate perception scores were high, the more likely that they would increase the scores of their climate perceptions of colleagues' InfoSec behaviours. In other words, employees' total number of InfoSec influencers can impact the contagion effect on their climate perceptions of colleagues' InfoSec behaviours. This explains why the weighted average contagion effect was not significant in Table F.1.

The results for the weighted average contagion and weighted total contagion effects also confirmed that these contagion effects did not influence employees' climate perceptions of direct supervisors' InfoSec behaviours. In other words, an employee's perception of direct supervisors' InfoSec behaviours did not increase as a result of receiving InfoSec influence from their colleagues whose scores of such perceptions were high. The summary of my modelling process and its results for the two contagion models is provided in Figure F.1.

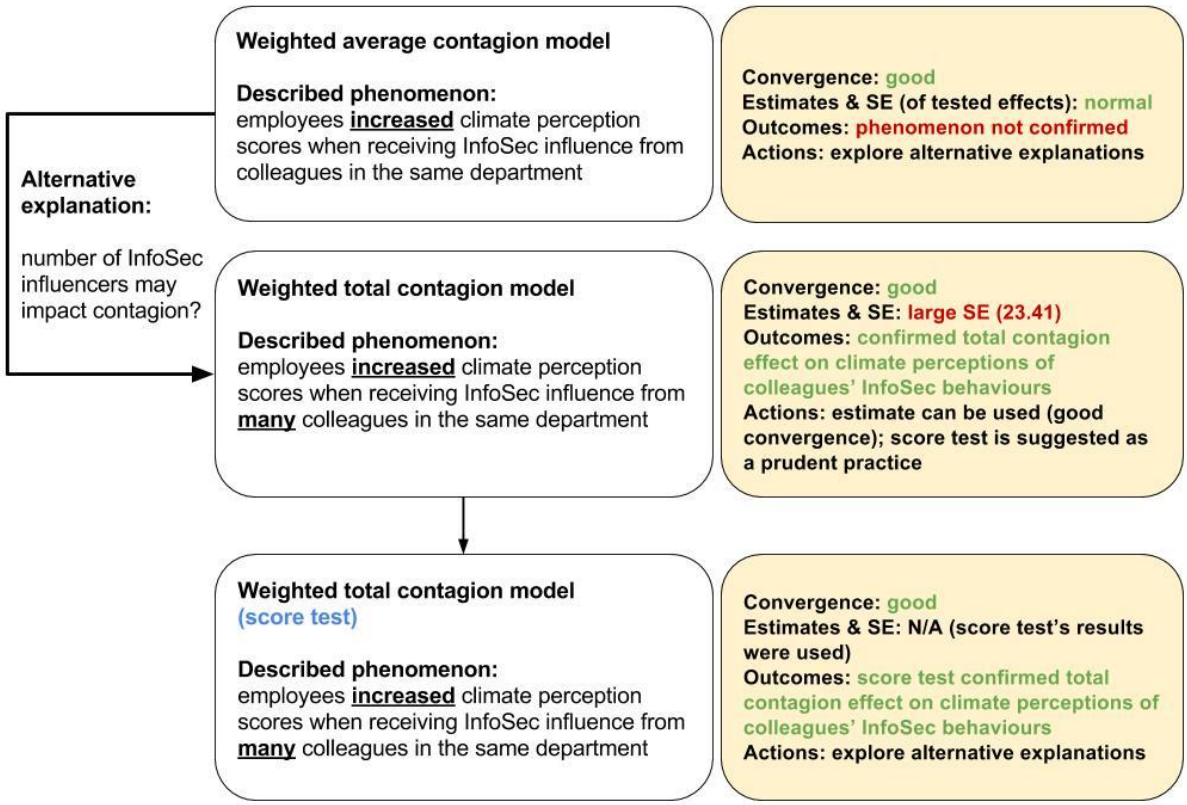


Figure F.1. The Modelling Process for the Contagion Models

Assimilation models

After I had investigated the impact of social influence on the formation of InfoSec climate perceptions via the contagion models, I explored alternative explanations by modelling the assimilation models. Any consistent findings of the assimilation models would further reinforce the findings about the impact of contagion on the formation of InfoSec climate as discussed previously.

Assimilation described the phenomenon where employees adjusted their perception scores to match with those of their colleagues in the same department who exerted InfoSec influence over them. With the knowledge that the total number of InfoSec influencers can impact social influence, I modelled the term weighted total assimilation effect and anticipated that it would achieve statistical significance. Table F.4 reports the results of this model.

Table F.4. Results of the Weighted Total Assimilation Model

Dynamics of InfoSec influence network	Estimate (Std. Error)	Converg. t-ratio
Rate of InfoSec influence	9.11*** (2.88)	0.03
Out-degree (likelihood of exerting InfoSec influence)	–7.68*** (0.67)	–0.17
Reciprocity	–0.8 (0.67)	–0.19
Transitivity (GWESP I -> K -> J)	1.94 (0.99)	–0.15
In-degree popularity	1.81*** (0.25)	–0.22
Out-degree activity	0.95*** (0.23)	–0.16
Out-in degree assortativity	–0.33*** (0.1)	–0.23
Structural equivalence (in terms of in-degree)	0.11*** (0.02)	0.27
Exerting InfoSec influence between employees in the same department	1.29*** (0.18)	–0.07
Female employees exerted InfoSec influence	–0.08 (0.15)	0.25
Female employees received InfoSec influence	–0.16 (0.18)	<0.01
Exerting InfoSec influence between employees of the same gender	0.11 (0.15)	–0.3
Old employees exerted InfoSec influence	0 (0.01)	–0.1
Old employees received InfoSec influence	0 (0.01)	–0.14
Exerting InfoSec influence between employees of similar age	–0.36 (0.56)	0.48
Employees with long tenure exerted InfoSec influence	0 (0.02)	–0.17
Employees with long tenure received InfoSec influence	0 (0.02)	–0.22
Exerting InfoSec influence between employees of similar tenure	0.51 (0.45)	0.34
Employees with high seniority exerted InfoSec influence	0.16 (0.26)	0.15
Employees with high seniority received InfoSec influence	0 (0.26)	–0.08
Exerting InfoSec influence between employees with the same seniority	–0.03 (0.25)	–0.23
Employees with champion status exerted InfoSec influence	0.44*** (0.14)	–0.06
Exerting InfoSec influence between employees with similar CIB	0.92 (1.67)	–0.14
Exerting InfoSec influence between employees with similar DSIB	–1.32 (0.9)	–0.01
Provision of work advice and/or organisational updates	1.44*** (0.32)	–0.01
Provision of personal advice and/or trust in expertise	1.49*** (0.28)	–0.03
Provision of InfoSec advice and/or troubleshooting support	0.99*** (0.33)	–0.28
Dynamics of climate perceptions of CIB	**Estimate (Std. Error)**	**Converg. t-ratio**
Rate of perception of CIB	1.78*** (0.32)	–0.03
Linear shape of perception of CIB	4.18 (3.44)	0.01
Quadratic shape of perception of CIB	–9.79*** (2.08)	–0.03
Total assimilation by InfoSec influence of same department employees	624.71*** (1.51)	<0.01
Effect of gender (female) on perception of CIB	–0.58 (4.06)	<0.01

Effect of age on perception of CIB	–0.51 (0.43)	–0.02
Effect of tenure on perception of CIB	–0.1 (0.64)	–0.01
Effect of seniority on perception of CIB	–2.65 (5.93)	0.01
Effect of champion status on perception of CIB	–7.47 (4.06)	0.01
Dynamics of climate perceptions of DSIB	**Estimate (Std. Error)**	**Converg. t-ratio**
Rate of perception of DSIB	2.73*** (0.59)	<0.01
Linear shape of perception of DSIB	0.72*** (0.25)	0.01
Quadratic shape of perception of DSIB	–0.35*** (0.09)	0.01
Total assimilation by InfoSec influence of same department employees	2 (2.92)	–0.01
Effect of gender (female) on perception of DSIB	–0.16 (0.23)	–0.02
Effect of age on perception of DSIB	–0.03 (0.02)	<0.01
Effect of tenure on perception of DSIB	0 (0.02)	0.01
Effect of seniority on perception of DSIB	–0.21 (0.26)	0.02
Effect of champion status on perception of DSIB	–0.12 (0.26)	<0.01

Note: *** denotes statistical significance; CIB = colleagues' InfoSec behaviours; DSIB = direct supervisors' InfoSec behaviours.

This weighted total assimilation model had many issues. First, its overall maximum convergence ratio was poor with a value of 2.5633, much larger than the recommended threshold of 0.25 (Ripley et al. 2017). This meant the model failed to produce the results that were reliable enough for interpretation. Second, the produced estimate for the weighted total assimilation effect was unusually large at 624.71. Given these results, I followed Ripley et al.'s (2017) advice and executed again the estimation process anticipating that the model would converge and the estimate and standard error of this effect would be stable enough for interpretation. However, the re-analysed model's results were even worse. The overall maximum convergence ratio of the model remained large at 1.838, which indicated the model failed to converge again. The estimate of the weighted total assimilation also inflated to 1133.88, which indicated the result could not be interpreted. These results implied that this weighted total assimilation effect could not be examined by the default estimation approach of the RSiena statistical package. For such a situation, Ripley et al. (2017) recommend using the score test as the only remedy.

I then applied the score test to examine while setting the result of the weighted total assimilation effect at zero, which established the null hypothesis that this effect would not impact employees' climate perceptions of colleagues' InfoSec behaviours. Likewise, I did the same

for the weighted total assimilation effect on the climate perceptions of direct supervisors' InfoSec behaviours. Examining the Chi-squared values and p-values produced by the score test would determine whether these null hypotheses could be rejected (i.e., the assimilation effects were significant). The score test's results are summarised in Table F.5.

Table F.5. Score Test Results for the Weighted Total Assimilation Effects

Effect	Chi-squared	p-value	One-sided normal variate	One-step estimate
Total assimilation by InfoSec influence of same department employees (perception of CIB)	18.46	<0.0001	4.30	13.55
Total assimilation by InfoSec influence of same department employees (perception of DSIB)	1.02	0.31	1.01	2.17

The Chi-squared value (18.46) and p-value (< 0.0001) of the weighted total assimilation effect on employees' climate perceptions of colleagues' InfoSec behaviours supported that this effect was significant. Moreover, the one-sided normal variate and one-step estimate of this effect both achieved positive values, 4.30 and 13.55 respectively, which indicated that the result of this effect would be positive (Lomi et al. 2011; Ripley et al. 2017). The score-tested results confirmed that employees tended to match their perceptions of colleagues' InfoSec behaviours with those of the InfoSec influencers in the same department, who exerted InfoSec influence over them. The weighted total assimilation effect on the climate perceptions of direct supervisors' InfoSec behaviours was not supported (Chi-squared = 1.02; p-value = 0.31). The use of the score test made the model achieve good convergence; overall maximum convergence ratio was 0.1243, indicating the results were reliable for interpretation. Finally, I applied the score test to determine the significance of the weighted average assimilation effect. Table F.6 summarises the results of this score test, which show that both average assimilation effects were not supported (p-values = 0.59).

Table F.6. Score Test Results for the Weighted Average Assimilation Effects

Effect	Chi-squared	p-value	One-sided normal variate	One-step estimate
Average assimilation by InfoSec influence of same department employees (perception of CIB)	0.29	0.59	0.54	18.24
Average assimilation by InfoSec influence of same department employees (perception of DSIB)	0.30	0.59	0.54	12.10

Overall, the results of these assimilation models were the same as those of the contagion models. Only the climate perception of colleagues' InfoSec behaviours was affected by social influence. Further, employees' total number of InfoSec influencers in the same department had impact on such social influence. The weighted total contagion and weighted total assimilation effects both achieved statistical significance in line with my expectation. A summary of my modelling process for the assimilation models is illustrated in Figure F.2.

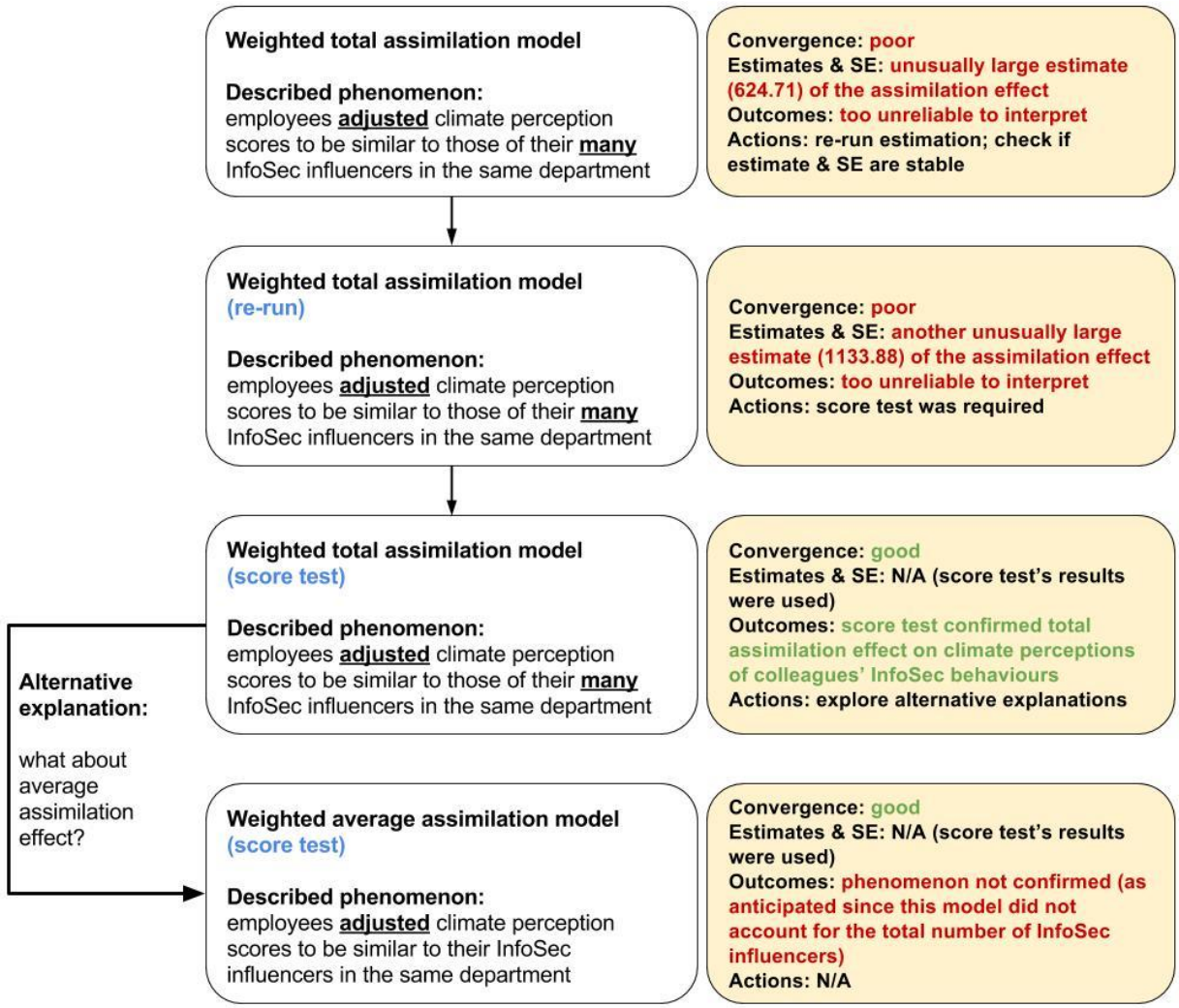


Figure F.2. The Modelling Process for the Assimilation Models

Evaluating Goodness-of-Fit

Before the models' results could be interpreted, I needed to check the extent to which the models can describe the actual phenomena. The goodness-of-fit of each model was assessed visually by examining the graphs that display the goodness-of-fit of the four network features which were the distributions of out-degree, in-degree, geodesic distance and triad census

(Ripley et al. 2017). Figures F.3, F.4, F.5 and F.6 show the graphs that evaluated the goodness-of-fit of the weighted average contagion model, the weighted total contagion model, the weighted average assimilation model and the weighted total assimilation model respectively.

The violin plots in the four smaller graphs within each figure presented the distributions of the four network features as simulated by the model. The graphs that showed acceptable goodness-of-fit had a red line (i.e., statistics of the observed InfoSec influence network) run through the violin plots and between the dotted band (i.e., the 95 per cent confidence interval calculated for the simulated statistics). Further, a p-value of larger than 0.05 at the bottom of each graph indicated acceptable goodness-of-fit of a feature. Overall, all four models achieved good goodness-of-fit for all features, indicating these models accurately described the observed InfoSec influence network and their results were reliable for interpretation.

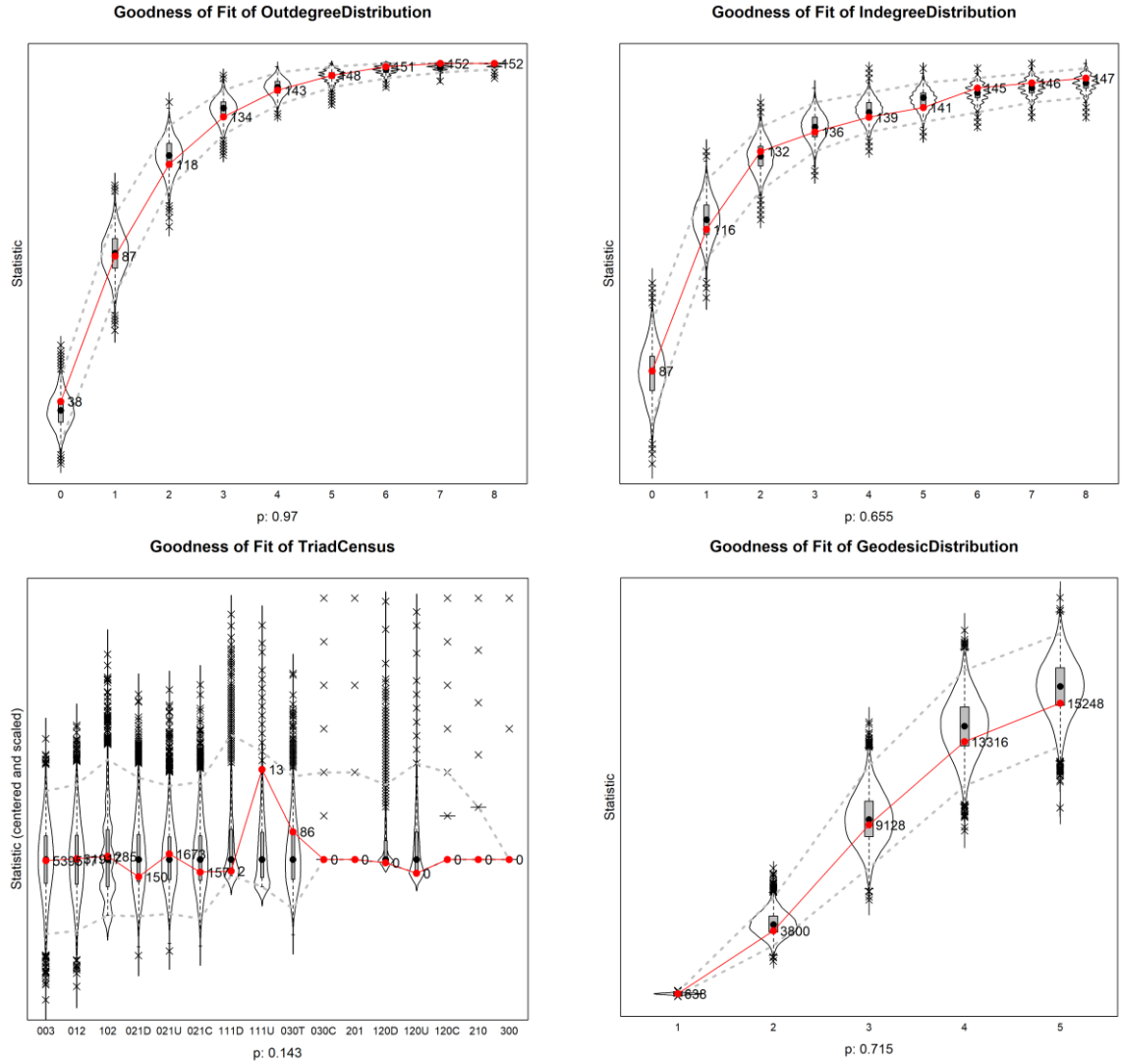


Figure F.3. Goodness-of-Fit of Weight Total Contagion Model

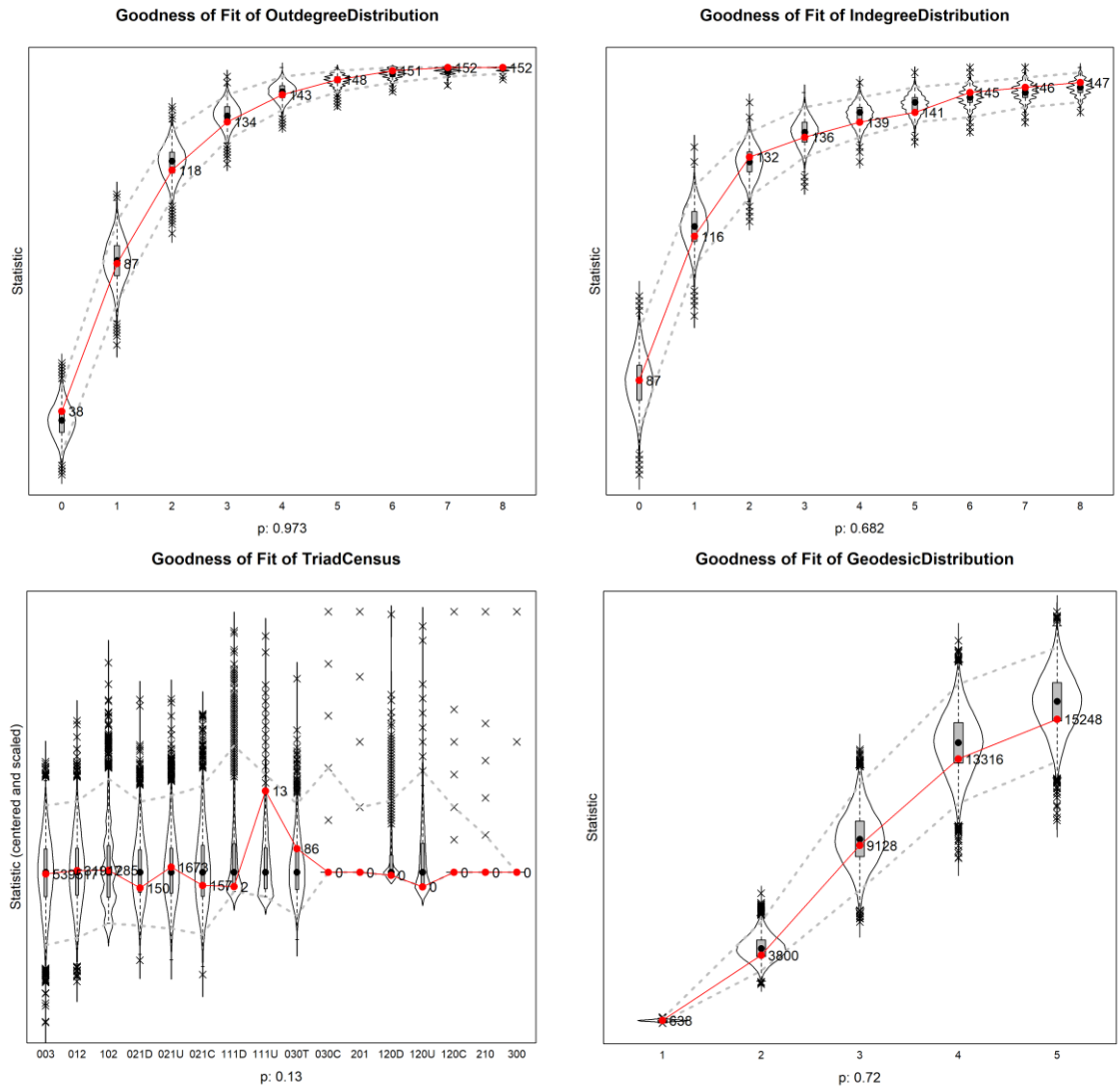


Figure F.4. Goodness-of-Fit of Weight Total Contagion Model

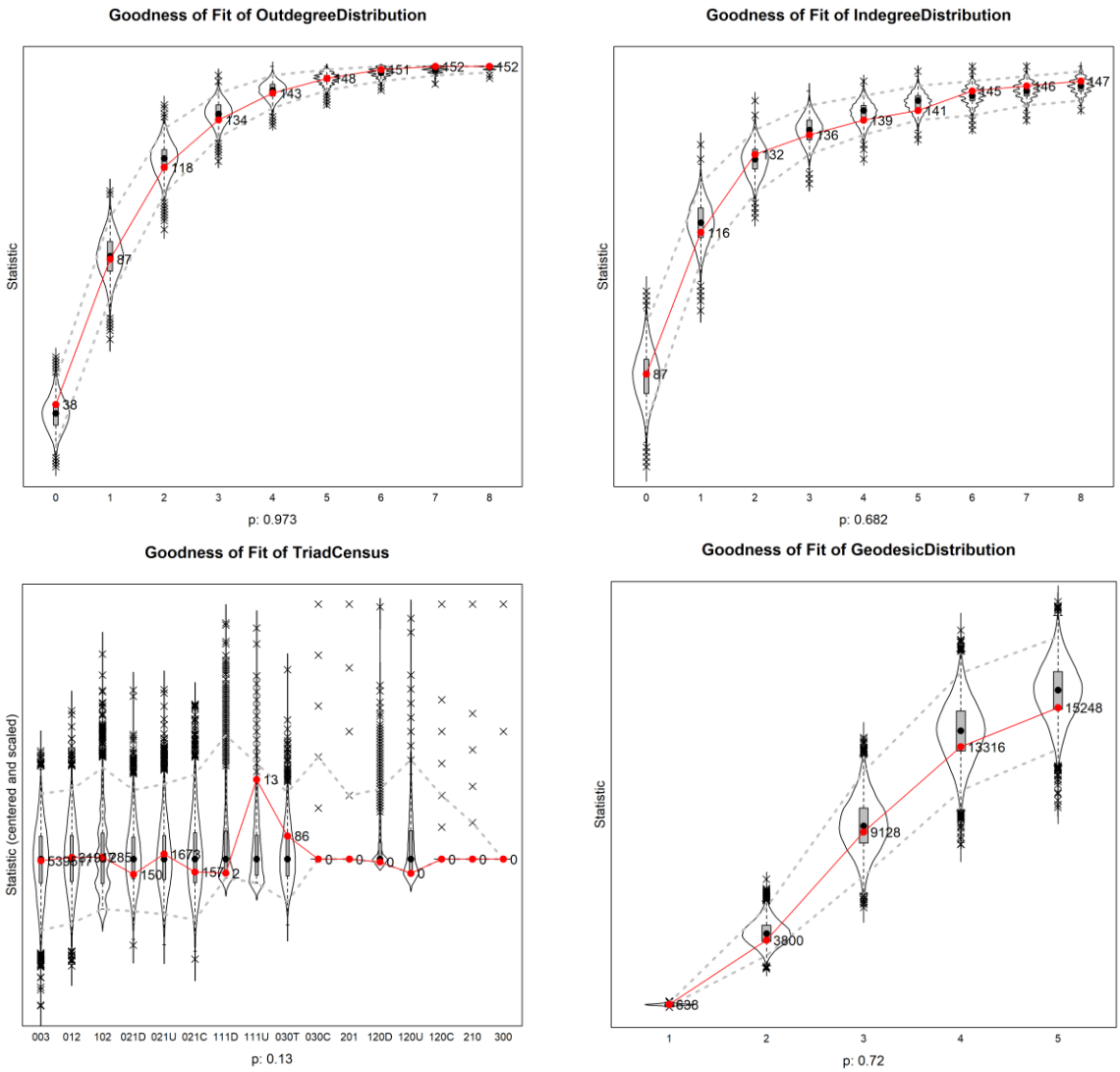


Figure F.5. Goodness-of-Fit of Weight Average Assimilation Model

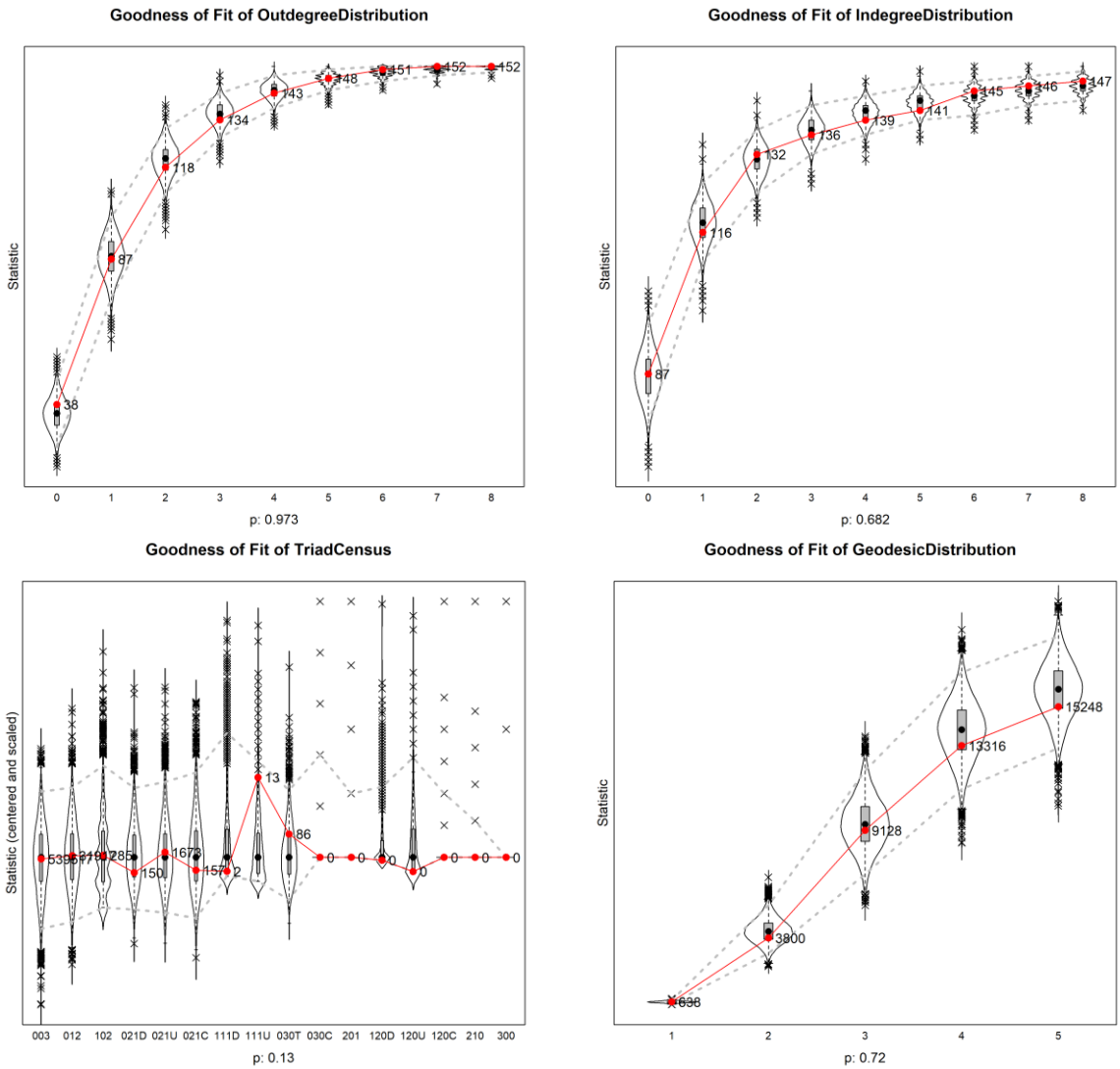


Figure F.6. Goodness-of-Fit of Weight Total Assimilation Model